Cybersecurity Law Casebook

Anna-Maria Osula
Bríd Ní Ghráinne
Dan Svantesson
David Kosař
Don Ferguson
Ivana Kudláčková
Jakub Klodwig
Jakub Vostoupal
Kateřina Uhlířová
Jan Kolouch
Veronika Žolnerčíková

Cybersecurity Law Casebook

Anna-Maria Osula
Bríd Ní Ghráinne
Dan Svantesson
David Kosař
Don Ferguson
Ivana Kudláčková
Jakub Klodwig
Jakub Vostoupal
Kateřina Uhlířová
Jan Kolouch
Veronika Žolnerčíková

General part

Sovereignty (Anna-Maria Osula, Dan Svantesson)

Jurisdiction (Anna-Maria Osula, Dan Svantesson)

International cybersecurity and cyber-defence

State Responsibility (David Kosař, Bríd Ní Ghráinne)

Use of Force (Ivana Kudláčková, Kateřina Uhlířová)

European and national cybersecurity

Critical Infrastructures (Don Ferguson)

Artificial Intelligence (Veronika Žolnerčíková)

Standardisation, Certification (Jakub Vostoupal)

Digital forensics

Digital Discovery (Jan Kolouch)

This book was supported by ERDF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

ISBN 978-80-210-9774-2 (online ; pdf)
ISBN 978-80-210-9773-5 (print)

Content

Sovereignty

Anna-Maria Osula, Dan Svantesson

1. Introduction

With its roots in the Peace of Westphalia, sovereignty is one of the core principle of international law. According to a widely accepted definition of the term in the 1928 Island of Palmas, "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State".[1] Furthermore, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations".[2]

Furthermore, sovereignty is often tied to territory, leading to the conclusion that the power of a State to exercise supreme authority over all persons and things within its borders is known as 'territorial sovereignty'.[3] The concept of territorial sovereignty relies on the opinion that sovereignty and jurisdiction can only be comprehended in relation to territory.4 Thus it has traditionally been claimed that the development of international law is based on the assumption that within an internationally recognised territorial framework the State has exclusive authority, and that '(b)etween independent States, respect for territorial sovereignty is an essential foundation of international relations.'[5] However, the traditional focus on territoriality is being challenged with our lives becoming increasingly digital, and shaped by the need for effective measures in fighting against cyber crime and collecting digital evidence.[6]

Despite debates over its exact meaning and scope, sovereignty is a concept which has established itself at the heart of the international legal system, and the sovereign State remains the ultimate member of the international community as well as the most important actor in the international legal system.[7]

2. Principle or a standalone rule?

While multiple international organisations[8] as well as several individual States have confirmed that international law applies in cyberspace, there continues to be a debate over whether sovereignty operates as a standalone rule of international law, the breach of which gives rise to

---

[1] Island of Palmas (Neth. v. U.S.), 2 RIAA 829, 838 (Perm. Ct. Arb. 1928).
[2] ICJ. Corfu Channel, para 202.
[3] Oppenheim, L. (1996). Oppenheim's International Law (9th ed, Longman) p. 382.
[4] Shaw, M. N. (2008). International Law (Cambridge University Press) p. 487.
[5] Corfu Channel (UK v Albania), 1949 ICJ 6, 35 (Apr 9) 35.
[6] See, e.g. Osula, A.-M. (2015). Transborder Access and Territorial Sovereignty. Computer Law and Security Review, 31 (6), pp. 719-735; Osula, A.-M. (2017). Remote search and seizure of extraterritorial data. (University of Tartu Press) pp. 1-96.
[7] M. Koskenniemi. (2005). From Apology to Utopia. (Cambridge: CUP) p. 236.
[8] See, e.g. UN GGE Res 71/237 (30 December 2015) UN Doc A/RES/20/237; North Atlantic Treaty Organization, 'Wales Summit Declaration'(issued by the Head of State and Government participating in the meeting of the North Atlantic Council in Wales (5 September 2015) para 72; Council of the European Union, "Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"(Council conclusions, 20 November 2017).

state responsibility, or whether sovereignty should be viewed as only a principle. To date, the traditional view has been to treat sovereignty as a substantive primary rule of international law, the breach of which is an internationally wrongful act. In turn, the occurrence of an internationally wrongful act is the legal basis for retaliation measures such as countermeasures.

However, the opponents of this view are putting forward the opinion that sovereignty is a principle of international law that may guide State interactions, but it does not amount to a standalone primary rule.[9] This view is now supported also by the United Kingdom.[10] According to this view, cyber operations may violate the principle of, for example, non-intervention, but not that of sovereignty as such. Nevertheless, the UK has made clear that "Online as well as everywhere else, the principle of sovereignty should not be used by states to undermine fundamental rights and freedoms and the right balance must be struck between national security and the protection of privacy and human rights."[11]

3. Threshold of breaching sovereignty

Sovereignty includes both an internal and an external element.[12] Internally, States assert legal authority over actors and activities taking place in cyberspace within the confines of their territory. More specifically, "[a] State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[13]

Externally, building on the assumption of viewing sovereignty as a rule, States must respect the sovereignty of other States.[14] However, the threshold on breaching sovereignty is far from settled. There are several elements to be taken into account when offering a legal assessment for a specific cased:

1. Physical damage or injury. Majority views cyber operations causing physical damage by remote means to another State a breach of its sovereignty.[15]
2. (A State organ) conducting cyber operations when physically present in the target State's territory. This is also viewed as a breach of sovereignty by the majority view.[16] There may be diverging views in the context of espionage.
3. Loss of functionality of the cyber infrastructure. Although majority may view causing loss of functionality as "damage", and thus a breach of sovereignty, no consensus could be achieved as on the precise threshold for a loss of functionality.[17] A parallel can also be made here with domestic criminal law which sees hindering the functionality of computer systems as a crime.[18]
4. Interference with data or services that are necessary for the exercise of "inherently governmental functions" such as elections.[19] See also discussions on the principle of non-intervention.

---

[9] Gary P. Corn and Robert Taylor. (2017). 'Sovereignty in the Age of Cyber' 111 AJIL Unbound 207, p. 208 (arguing that sovereignty is 'a principle of international law that guides state interactions').
[10] Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century
[11] Id.
[12] James Crawford, Brownlie's Principles of Public International Law (OUP 2012) p 448.
[13] Schmitt, M. gen. ed. (2017) Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations, rule 2.
[14] Tallinn Manual 2.0, rule 4.
[15] Tallinn Manual 2.0, commentary to rule 4, para 11.
[16] Tallinn Manual 2.0, commentary to rule 4, para 6.
[17] Tallinn Manual 2.0, commentary to rule 4, para 13.
[18] See, e.g. the Budapest Convention.
[19] Tallinn Manual 2.0, commentary to rule 4, para 15.

5. Usurpation of "inherently governmental functions", such as exercise of law enforcement functions in another State's territory without justification. There are opposing views on whether carrying out inherently governmental functions such as conducting criminal investigations (without causing damage and loss of functionality) should be viewed as a breach of sovereignty. Although Tallinn Manual would appear to be representing the side which labels, e.g. remote search and seizure measures for accessing the data on the territory of another State as breaching the other States sovereignty, there are several strong arguments regarding current State practice which support a contrary view.[20]

4. Cases

- Island of Palmas (Neth. v. U.S.), 2 RIAA 829, 838 (Perm. Ct. Arb. 1928).
- Corfu Channel

[20] See examples for such domestic regulation in, e.g. Osula, A.-M. (2017). Remote search and seizure of extraterritorial data. (University of Tartu Press).

Jurisdiction

Dan Svantesson, Anna-Maria Osula

1. General

The concept of jurisdiction is multifaceted and complex, and as noted by the High Court of Australia: "It is a generic term […]. It is used in a variety of senses, some relating to geography, some to persons and procedures, others to constitutional and judicial structures and powers."[21]

At its core, the concept of jurisdiction delineates state powers of various kinds. Inevitably this adds a political dimension that rarely is helpful for the pursuit of legal clarity, certainty and appropriate nuances. Also, since much of the law relating to jurisdiction has developed through the decisions of national courts applying their national laws, sometimes irrespective of their compatibility with international law, the influence of national jurisprudence has contributed to the uncertainty surrounding many matters of jurisdiction.[22]

2. Types of jurisdiction in public international law

In public international law, jurisdictional claims traditionally fall under the categories of

1. legislative (or prescriptive) jurisdiction – i.e., the power to make its law applicable to the activities, relations or persons;
2. adjudicative (or judicial) jurisdiction – i.e., the power to subject persons or things to the process of its courts or administrative tribunals; or
3. enforcement jurisdiction – i.e., the power to induce or compel compliance or punish noncompliance with its laws or regulations.

A fourth category – investigative jurisdiction – is increasingly recognized as well.[23] While investigative measures have traditionally been treated as an aspect of enforcement jurisdiction, such measures radically differ from other categories of conduct (such as arrests on foreign soil) that are also classified as claims of enforcement jurisdiction. There is therefore little merit in grouping such distinct matters under one heading. Treating investigative jurisdiction as a distinct category is of particular significance in the context of cyber security and investigation of transborder crime.

At any rate, the neat categorization outlined above is somewhat of an illusion. To see that this is so, you need only to ask yourself to which category of jurisdiction the seminal *Lotus* case[24] (included below) relates to. Even the judges in that case do not agree on that issue.

Furthermore, it is often assumed that the impacts of claims of enforcement jurisdiction are necessarily more severe than the consequences of legislative jurisdiction or adjudicative jurisdiction claims. Yet this is an oversimplification. Ultimately, the impact of each jurisdictional claim must be assessed regardless of category; and the greater the potential for a jurisdictional

[21] Lipohar v R [1999] HCA 65, para 78 (per Gaudron, Gummow and Hayne JJ).
[22] Oppenheim, L. Oppenheim's International Law (9th ed, Longman, 1996) p. 457.
[23] See e.g.: Lawson v Accusearch Inc dba Abika.com [2007] 4 FCR 314 and Weltimmo s.r.o.v. Nemzeti Adatvédelmi és Információszabadság Hatóság (Case C- 230/ 14). See also: Svantesson, D. (2012). Extraterritoriality in the context of data privacy regulation. *Masaryk University Journal of Law and Technology* 7(1) 87-96, 92-93. Retrieved from https://journals.muni.cz/mujlt/article/viewFile/2628/2192
[24] SS 'Lotus' (France v Turkey) (1927) PCIJ Series A, No 10.

claim has to interfere with the sovereignty of another state, the greater the reason to limit the exercise of jurisdiction.

3. When states may or must claim jurisdiction

In certain situations, states are obligated to claim jurisdiction. This is an important aspect of international law aimed at avoiding gaps and ensuring access to justice. However, most discussions of jurisdiction are centred around the extent to which international law imposes limitations on state claims of jurisdiction. A common thread of today's discussions in this context is an exaggerated, and arguably misguided, focus on territoriality.

The two sources most commonly relied upon here are the (in)famous 1927 *Lotus* case[25] and the widely cited, but poorly understood, *Harvard Draft Convention on Jurisdiction with Respect to Crime 1935*[26] (partially included below) – both seen to put the supremacy of the territoriality principle beyond question. With a sleep-walking like acceptance, these authorities are treated as clear, exhaustive and almighty.

However, those who have truly studied jurisdiction in detail generally take a different view. For example, Ryngaert[27] and Mann[28] have both questioned whether the *Lotus* decision remains good law. And as has been illustrated elsewhere, pretty much every aspect of how we classify jurisdictional claims – including the distinction between jurisdiction under public international law and jurisdiction under private international law, as well as the distinction between territorial and extraterritorial jurisdiction – is less settled than it often is portrayed as being and may usefully be called into question.[29]

At any rate, if we adopt the conventional classification of jurisdiction; legislative, adjudicative and enforcement, it may be said that convention suggest that legislative (or prescriptive) jurisdiction is governed by the following well-known principles, first articulated in the *Harvard Draft Convention on Jurisdiction with Respect to Crime 1935* (with the arguable addition of the 'effects doctrine'):

1. Territoriality principle
2. Nationality Principle
3. Passive personality principle
4. Protective principle
5. Universality principle.

An insight into some form of mainstream view of the applicable international law on enforcement jurisdiction can be gleaned from the conclusions reached by the group of eminent experts who, in 2017, produced the Tallinn Manual 2.0:

"States generally do not possess enforcement authority outside their territory. Rather, such jurisdiction is an exclusive attribute of sovereignty and, as such, may only be exercised

[25] SS 'Lotus' (*France v Turkey*) (1927) PCIJ Series A, No 10.
[26] 'Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935' (1935) 29 Supp Am J Intl L 443.
[27] Ryngaert, C. (2015) *Jurisdiction in International Law.* 2nd ed. Oxford: Oxford University Press, p. 34.
[28] Mann, F. (1996) The doctrine of Jurisdiction in International Law. In Karl M Meesen (ed), *Extraterritorial Jurisdiction in Theory and Practice*. Kluwer Law International, p. 66.
[29] See further: Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, in particular pp. 159-170.

extraterritorially with the consent of the State in which the jurisdiction is to be exercised or pursuant to a specific allocation of authority under international law."[30]

The detailed rules for adjudicative (or judicial) jurisdiction are disputed.[31]

Finally, while the criteria for investigative jurisdiction are still crystallising, it already seems clear that they are not focused on territoriality in the manner convention sets criteria for the other types of jurisdiction.[32] Rather, at least moving forward, attention is primarily directed at three criteria:

1. Substantial connection;
2. Legitimate interest in obtaining the specific data sought; and
3. Interests of others.[33]

4. Territorial, and extraterritorial, jurisdictional claims

A distinction is often drawn between territorial and extraterritorial jurisdictional claims. For example, the nationality principle can be employed in order to extend a state's material jurisdiction to its citizen located in another state, or the subjective and objective territoriality principles can be applied when part of the offence has taken place in a foreign territory.

Unfortunately, the implications of extraterritorial jurisdictional claims are often overstated with regard to international law. In fact, the territorial/extraterritorial dichotomy is sometimes misused as shorthand for distinguishing between legitimate and illegitimate claims of jurisdiction. However, just as there may be perfectly legitimate extraterritorial claims of jurisdiction under international law, there may be questionable territorially-based claims of jurisdiction as well.

In addition, under international law there is no clear consensus on how to define a jurisdictional claim as extraterritorial. As illustrated in the 2018 *Microsoft Warrant* case,[34] for example, even legal systems that include an express presumption against extraterritoriality lack a clear definition of extraterritoriality in the online context. This further undermines the usefulness of the binary territorial/extraterritorial dichotomy as a tool for addressing cross-border legal challenges on the Internet.

5. Briefly about the relationship between sovereignty and jurisdiction

Convention may have us believe that the scope of jurisdiction is determined by the (territorial) reach of sovereignty. However, few steps can be taken in such a direction without getting tangled in conflicting wisdoms. To bring forward just one illustration: if the scope of jurisdiction is determined by the reach of sovereignty, and sovereignty is delineated by reference to territorial borders, how do we explain recognised forms of extraterritorial jurisdiction, such as jurisdictional claims based on the nationality of an offending party?

More generally, as noted by Khan:

---

[30] Schmitt, M. gen. ed. (2017) Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations, pp. 52-53.

[31] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, in particular pp. 160-163.

[32] See e.g.: the US' Clarifying Lawful Use of Overseas Data Act ('CLOUD Act') and the EU's proposed e-evidence Directive and Regulation.

[33] https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf.

[34] United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2).

[I]n recent years there are increasing signs that the traditional and rather categorical symbiosis between territory and power may no longer lay a legitimate claim for exclusivity. This is hardly deplorable since from an international law perspective, possession and transfer of territory have never been considered an end in itself. *L'obsession du territoire* of modern States was always meant to serve people, not vice versa.[35]

All this illustrates that, while there are obvious *indirect* links between jurisdiction and sovereignty, there is no necessary *direct* link between these concepts as such. In response to this, some will hasten to drag forward the old argument that jurisdiction ultimately depends on enforcement. However, it should be seriously questioned whether people who do so have really thought through the implications of what they then are saying. Surely, we need to distinguish between law, on the one hand, and brute power, on the other hand, even if doing so means that we have to accept (a) that law can be of value even if it cannot be enforced, and (b) that not all enforcement actions are legitimate?

6. A look towards the future

It has long been recognised that a territoriality-centred thinking on jurisdiction is ill-equipped to deal with the online environment. This is particulary relevant for a highly fluid context of cyber security. Against this background, attempts at developing better models have emerged. Under one such attempt, the following jurisprudential core for jurisdiction has been identified:

"In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where:

(1) there is a substantial connection between the matter and the State seeking to exercise jurisdiction;

(2) the State seeking to exercise jurisdiction has a legitimate interest in the matter; and

(3) the exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests."[36]

The application of this framework has been discussed specifically in relation to cyber security in a recent book.[37]

7. Cases

- SS 'Lotus' (France v Turkey) (1927) PCIJ Series A, No 10
- Barcelona Traction (Belgium v Spain) ICJ Rep 42 (1970)
- Corfu Channel [1949] ICJ Rep 4
- Nottebohm (Liechtenstein v Guatemala) ICJ Rep 4 et seq (1955)
- In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, No 14-2985, 2016 WL 3770056 (2d Cir July 14, 2016)
- Democratic Republic of Congo v. Belgium (2000) ICJ Rep 182 (the Arrest Warrant Case)

[35] See, eg, Khan, D.E. (2012) Territory and Boundaries. In Bardo Fassbender and Anne Peters (eds), *The Oxford Handbook of The History of International Law*. Oxford: Oxford University Press, p. 248 (footnote omitted).
[36] Svantesson, D. (2015) A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft. 109 *American Journal of International Law Unbound* 69 https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft.
[37] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing, pp. 155-187.

- Attorney-General of the Government of Israel v Eichmann (1961) 36 ILR 5 (District Court of Jerusalem)
- Jurisdictional Immunities of the State (Germany v Italy) [2012] ICJ Reports
- Lawson v Accusearch Inc dba Abika.com [2007] 4 FCR 314

State Responsibility

Bríd Ní Ghráinne, David Kosař

1. Introduction

Every internationally wrongful act by a subject of international law entails its international responsibility.[38] The law of state responsibility sets out the general framework under international law for the state to be considered responsible for wrongful actions or omissions, and the legal consequences which flow therefrom.[39] Thus the focus in the field of state responsibility is on 'second-order issues', that is, the procedural or other consequences flowing from a breach of a substantial rule of law.[40]

As states are the primary subjects of international law, the law of state responsibility is the most fully developed branch of responsibility and is therefore the principal focus of this chapter.[41] As the responsibility of other actors in international law is comparatively underdeveloped, it is considered only in passing.

The structure of this chapter will be as follows. Section two sets out the scope of state responsibility. Section three sets out the basic elements of state responsibility: attribution, breach, and circumstances precluding wrongfulness. Sections four and five set out the invocation and consequences of state responsibility, respectively. Section six applies the principles of State Responsibility to the cybersecurity context, and section seven concludes.

2. The Scope of State Responsibility

The rules of state responsibility are set out in the International Law Commission's (ILC) Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA). The Articles are the product of more than forty years' work by the ILC on this topic and they represent both codification and progressive development of the law of state responsibility.[42]

Article 1 of ARSIWA provides the general rule, widely supported in practice,[43] that every internationally wrongful act of a state entails the international responsibility of that state. An internationally wrongful act may consist of one or more actions or omissions or a combination of both actions and omissions.[44] It is also important to note that a state that directs and/ or coerces another state to commit an internationally wrongful act may also trigger the responsibility of the directing/coercing state.[45]

---

[38] See the dictum of the *Permanent Court of International Justice in Factory at Chorzow, jurisdiction, judgment No B, 1927, PClj, Ser A, No 9* at p 21: 'It is a principle of international law that the breach of an engagement involves an obligation to make reparation'.
[39] International Law Commission, 'Draft articles on the responsibility of international organizations, with commentaries', 2001, Supplement No. 10 (A/56/10), chp.IV.E.1, available at https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
[40] Malcolm Shaw, *International Law* (CUP 2008), 566.
[41] James Crawford and Simon Olleson, 'The Nature and Forms of International Responsibility' in Malcolm Evans, *International Law* (2003), 445.
[42] Ibid, 448.
[43] International Law Commission, n 39, 63.
[44] International Law Commission, n 39.
[45] International Law Commission, n 39, Articles 17-19.

Whether there has been an internationally wrongful act depends primarily on the legal obligations of the relevant state. There is no such thing as a uniform code of international law, reflecting all the obligations of states. Each state has its own unique patchwork of legal obligations reflecting, inter alia, the organisations which it has joined and the treaties it has become a party to.[46] The field of state responsibility does not attempt to define the content of the primary international obligations, the breach of which gives rise to responsibility. This is the role of the primary rules.[47] Rather, the field of state responsibility, put simply, amounts to a general international law of wrongs.[48] At a domestic level, it might be likened to the law of torts, or the law of obligations. The international law of state responsibility sets out the general underlying concepts of state responsibility – attribution, breach, excuses, and consequences – which help us to identify under what circumstances a state's actions has given rise to its international legal responsibility. Each of these elements will be analysed in turn below.

3. The Elements of State Responsibility

In order for there to be an internationally wrongful act, there must be (a) an act that is attributable to a state under international law; (b) that act constitutes a breach of an international obligation of the state; and (c) an absence of any valid justification for the act, also termed 'circumstances precluding wrongfulness (CPW).'

3.1. Attribution

Article 2 of ARSIWA provides that there is an internationally internationally wrongful act of a state when conduct consisting of an action or omission is attributable to the state under international law and constitutes a breach of an international obligation of the state.[49] A State, as an abstract entity, cannot 'act'[50] of itself. Like corporations in national law, states act through organs or agents. Attribution (also sometimes referred to as imputability) is the legal fiction which equates the actions or omissions of individuals to the state.[51] The rules of attribution are also codified in customary international law.[52]

According to Article 4 ARSIWA, a state is generally liable for the conduct of its organs.[53] The ICJ in the *Genocide* case regarded this rule as 'one of the cornerstones of the law of state responsibility'.[54] The scope of state responsibility for acts of its organs or officials is broad. There is no distinction based on the level of seniority of the relevant officials – as long as they are acting in their official capacity, responsibility may be triggered.[55] Thus the concept of organs covers legislative, executive officials, and courts at all levels.[56] Shaw notes that this broad definition encourages states to exercise greater control over its various departments and representatives.[57]

---

[46] Crawford and Olleson, n 41, 447.
[47] International Law Commission, n 39.
[48] Crawford and Olleson, n 41, 447.
[49] International Law Commission, n 39.
[50] International Law Commission, n 39, 35; Crawford and Olleson, n 41, 453; Shaw, n 40, 572.
[51] Shaw, n 40, 572.
[52] Application of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, ICJ Reports 2007, p 43 [385].
[53] Salvador Commercial Company, UNRIAA, vol. XV (Sales No. 66.V.3), p. 455 (1902); Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion, ICJ Reports 1999, p. 62, Certain German Interests in Polish Upper Silesia, Merits, Judgment No. 7, 1926, P.C.I.J., Series A, No. 7.
[54] Application of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), n 52, [385].
[55] Crawford and Olleson, n 41, 454.
[56] International Law Commission, n 39, 41.
[57] Shaw, n 40, 571.

Article 5 ARSIWA provides that the conduct of a person or entity which is not an organ of the state but which is empowered by the law of that state to exercise elements of governmental authority may also be attributed to the state, provided the person or entity is acting in that capacity at the relevant time.[58] This provision is intended to cover public corporations, semi- public entities, public agencies of various kinds and even, in special cases, private companies, provided that in each case the entity is empowered by the law of the State to exercise functions of a public character normally exercised by State organs, and the conduct of the entity relates to the exercise of the governmental authority concerned. For example, in some states, private security firms may be contracted to act as prison guards and in that capacity, may exercise public powers such as powers of detention and discipline pursuant to a judicial sentence or to prison regulations. In addition, private or State-owned airlines may have delegated to them certain powers in relation to immigration control or quarantine.[59]

Article 6 ARSIWA provides that the conduct of an organ placed at the disposal of a state by another state shall be considered an act of the former state under international law if the organ is acting in the exercise of elements of the governmental authority of the state at whose disposal it is placed. This would, for example, cover a section of the health service or some other unit placed under the orders of another country to assist in overcoming an epidemic or natural disaster, or judges appointed in particular cases to act as judicial organs of another State such as the UK Privy council acting as the highest judicial body for certain Commonwealth countries.[60]

3.2. Ultra vires acts

Article 7 ARSIWA provides the conduct of an organ or of a person or entity empowered to exercise elements of governmental authority shall be considered an act of the state under international law if acting in that capacity, even if it exceeds its authority, violates rules, or contravenes instructions. Shaw notes that this seems to lay down an absolute rule of liability.[61] The reasoning for this absolute rule is to prohibit abuse, as were it not for this rule there would be no practical way of proving that the agent had or had not acted on orders received.[62] The rule was applied in the *Caire* case, where a French national in Mexico was murdered by two Mexican officers after he refused their demands for money. The French-Mexican Claims Commission stated that even though these officers acted outside their authority, Mexico was responsible because the two officers 'acted in their capacity as officers and used the means placed at their disposition by virtue of that capacity.'[63] This was reaffirmed by the Inter-American Court of Human Rights in the *Velásquez Rodríguez* case:

This conclusion [of a breach of the Convention] is independent of whether the organ or official has contravened provisions of internal law or overstepped the limits of his authority: under international law a State is responsible for the acts of its agents undertaken in their official capacity and for their omissions, even when those agents act outside the sphere of their authority or violate internal law.[64]

[58] International Law Commission, n 39, Article 5.
[59] International Law Commission, n 39, 42.
[60] International Law Commission, n 39, 44, 45.
[61] Shaw, n 40, 789.
[62] International Law Commission, n 39, 45.
[63] Caire (France V Mexico) (1929) 5 RIAA 516, 530.
[64] *Velásquez-Rodríguez v. Honduras*, Inter-American Court of Human Rights, 1989, Series C, No. 7, pp. 34, 52; 95 ILR, p. 306.

3.3. Attribution of private acts to the state

Private acts are generally not attributable to the state.[65] However, such acts may be attributable to the state if: (i) private persons were acting under the instructions of, or control of that state; (ii) where an insurrectional movement subsequently becomes the government of that state; (iii) if the state adopts private acts as its own.

With regard to situation (i); Article 8 ARSIWA provides that a state is responsible for the acts of private persons who were acting under the instructions of, or control of, that state. The Commentary to ARSIWA emphasizes that 'such conduct will be attributable to the state only if it directed or controlled the specific operation and the conduct complained of was an integral part of the operation'.[66] Although case law subsequent to the publication of ARSIWA has put forward two different understandings of what 'directed or controlled' the specific operation means, it is generally agreed that Article 8 embodies an 'effective control test.'

The 'effective control' test was set out by the ICJ in *Nicaragua v USA*. The ICJ held that the United States was responsible for the 'planning, direction and support' given by the United States to Nicaraguan operatives. The Court then had to consider the broader claim of whether actions by the guerilla contras in breach of international humanitarian law (killing of prisoners, indiscriminate killing of civilians, torture, rape and kidnapping) could be attributed to the US, which had financed and equipped the force. The Court answered this question in the negative. It required for such attribution to arise, 'it would in principle have to be proved that that state had effective control of the military or paramilitary operation in the course of which the alleged violations were committed.'[67] By such 'effective control ', the Court meant that the US should have 'directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State'.[68] It seems clear from these words that by 'effective control' the Court intended either (1) the issuance of directions to the contras by the US concerning specific operations (indiscriminate killing of civilians, etc.) or (2) the enforcement by the US of each specific operation of the contras, i.e. forcing the rebels to carry out those specific operations.[69]

The second approach -the 'overall control' test – was set out by the ICTY in the *Tadic* case.[70] The Tribunal approved the test of 'overall control going beyond the mere financing and equipping of such forces and also involving the participation in the planning and supervision of military responsibility.'[71] This was a more flexible approach than that of *Nicaragua*, as it accepts that the degree of control might vary according to the circumstances and a high threshold might not always be required.[72]

By the time the *Genocide* case came before the ICJ in 2007, the Court was faced with two possible applicable tests in determining whether the conduct of the Bosnian Serb forces and paramiltary groups was attributable to the FRY. The Court held that the 'overall control' test proposed by the ICTY in *Tadic* was unpersuasive and maintained the 'effective control' test adopted in *Nicaragua*. It noted that *Tadic* did not concern issues of state responsibility as it was before a criminal tribunal, and that the 'overall control' test was inappropriate in such contexts:

---

[65] International Law Commission, n 39, 38.
[66] International Law Commission, n 39, 47.
[67] Military and Paramilitary Activities in and against Nicaragua, Merits, Judgment (Nicaragua v United States of America), ICJ Reports 1986, p 14, [115].
[68] Ibid, [109]; [115].
[69] Antonio Cassese, 'The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia', (2007) 18(4) European Journal of International Law 649, 653.
[70] Case No IT-94-1-A, *Prosecutor v Tadic*, *Judgment of 15 July 1999*, (1999) 38 ILM 1518.
[71] Ibid [145].
[72] Ibid, [117].

[The 'overall control' test has the major drawback of broadening the scope of Stat responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf… [T]he overall control test stretches too far, almost to breaking point, the connection with which must exist between the conduct of a State's organs and its international responsibility.[73]

The ICJ thus held that the test under customary law was that reflected in Article 8 ARSIWA whereby the state would be responsible for the acts of private persons or groups where an organ of the state gave the instructions or provided the direction pursuant to which the perpetrators of the wrongful act acted or where it exercised effective control over the action during which the wrong was committed.

Situation (ii) as set out above is dealt with in Article 10 ARSIWA. This provision provides that conduct of a movement which becomes the new government or establishes a new state will be attributed to the respective state under international law. Crawford and Olleson describe this rule as 'anomalous' as it determines the 'attribution of conduct not by events at the time of that conduct but by reference to later contingencies, i.e. the success or failure of the revolt or secession.'[74] It was applied in the *Yeager* case,[75] which concerned the period immediately after the revolution in Iran in 1979. The claimant in this case had been detained for several days by 'revolutionary guards' and then evacuated from the country. The Tribunal held that, although the guards were not recognized under internal law as part of the State, they were in fact exercising public functions in the absence of the previous State apparatus: Iran was thus held responsible for their acts.

Finally, a state's responsibility may also become engaged as per situation (iii) above where it subsequently adopts the actions of private actors as its own. In the *Tehran Hostages* case, the ICJ held that although the students who initially took control of the US embassy in Tehran were not acting as agents of Iraq, the subsequent statement of Ayatollah Khomeini endorsing the occupation of the embassy translated the occupation of the Embassy and detention of the hostages into acts of Iran:

The policy thus announced by the Ayatollah Khomeini, of maintaining the occupation of the Embassy and the detention of its inmates as hostages for the purpose of exerting pressure on the United States Government was complied with by other Iranian authorities and endorsed by them repeatedly in statements made in various contexts. The result of that policy was fundamentally to transform the legal nature of the situation created by the occupation of the Embassy and the detention of its diplomatic and consular staff as hostages. The approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State.[76]

The Court also found that Iran was responsible for its omission of failure to protect the embassy from the mob.

3.4. Breach of an International Obligation of the State

There is a breach of an international obligation by a State when an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character.[77] In determining whether given conduct attributable to a State constitutes a breach of its international

[73] *Ibid,* [406].
[74] Crawford and Olleson, n 41, 457.
[75] Yeager (1987), 82 ILR 178.
[76] United States Diplomatic and Consular Staff in Tehran, Judgment, ICJ Reports 1980, p. 35, [74].
[77] International Law Commission, n 39, Article 12.

obligations, the principal focus will be on the primary international law obligation concerned.[78] A 'breach' of international law may include 'non-execution of international obligations', 'acts incompatible with international obligations', 'violation of an international obligation', 'breach of an engagement' or acts 'contrary to the treaty right[s] of another state.'[79] A breach may arise of any provision of international law, regardless of its source.[80] Finally, it is important to note that it is international law that determines what constitutes an internationally wrongful act, regardless of any provisions of domestic law.[81] Thus a state cannot invoke domestic law as justification for an internationally wrongful act.[82]

Whether the state needs to be at fault in order to give rise to responsibility in international law is not so clear-cut. The principle of objective responsibility (the so-called 'risk' theory) maintains that the liability of the state is strict. Once an unlawful act has taken place, which has caused injury and which has been committed by an agent of the state, that state will be responsible in international law to the state suffering the damage irrespective of good or bad faith.[83] This approach can be contrasted with the subjective responsibility concept (the 'fault' theory) which emphasises that an element of intentional or negligent conduct on the part of the person concerned is necessary before his state can be rendered responsible for the breach of international law.[84] The relevant cases and academic opinions are divided on this question, although the majority tends towards the strict liability, objective theory of responsibility.[85]

ARISWA takes a more nuanced approach.[86] Under Articles 2 and 12, State responsibility does not require fault before an act or omission may be characterized as internationally wrongful. However, the interpretation of the relevant primary obligation in a given case may well lead to the conclusion that fault is a necessary condition for responsibility in relation to that obligation, having regard to the conduct alleged.[87]

Similarly, there has been a debate concerning the role of harm or damage in the law of State responsibility. Some authors have claimed that the State must have suffered some form of actual harm or damage before responsibility can be engaged.[88] Once more, the ILC Articles leave the question to be determined by the relevant primary obligation: there is no general requirement of harm or damage before the consequences of responsibility come into being.[89] In some circumstances, the mere breach of an obligation will be sufficient to give rise to responsibility; for instance, even a minor infringement of the inviolability of an embassy or consular mission will give rise to responsibility. On the other hand, in the context for example of pollution of rivers, it is necessary to show some substantial impact on the environment or on other uses of the watercourse before responsibility will arise.[90]

---

[78] International Law Commission, n 39, 54.
[79] International Law Commission, n 39, 35.
[80] International Law Commission, n 39, 55.
[81] International Law Commission, n 39, Article 3, 54-55.
[82] International Law Commission, n 39, Article 3; Bríd Ní Ghráinne and Aisling McMahon, 'Abortion in Northern Ireland and the European Convention of Human Rights: Reflections from the UK Supreme Court,' 68(2) International and Comparative Law Quarterly 477; Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 VCLT 331.
[83] Shaw, n 40, 570.
[84] Shaw, n 40, 570.
[85] Crawford; and Olleson, n 41, 462.
[86] Crawford and Olleson , n 41, 462.
[87] International Law Commission, n 39, 34.
[88] Brigitte Bollecker- Stern, *Le prejudice dans la theorie de la responsibilite internationale* (Pedone 1973), as cited in Crawford and Olleson, n 41, 460.
[89] International Law Commission, n 39, 36.
[90] Crawford and Olleson, n 41, 460.

A corollary of this position is that there may have been a breach of international law but no material harm may have been suffered by another State or person in whose interest the obligation was created. In such cases courts frequently award merely declaratory relief on the ground that nothing more is required. The aim of asserting responsibility in such cases may be for the future, to avoid repetition of the problem, rather than to obtain compensation for the past.[91]

3.5. Circumstances Precluding Wrongfulness

Even where conduct may be attributable to a state, and in breach of that state's obligation, the state will not necessarily incur responsibility under international law. The State may be able to rely on some defence or excuse: in the ILC's Articles these are collected under the heading of 'Circumstances precluding wrongfulness'.[92] CPWs do not annul or terminate the obligation; rather they provide a justification or excuse for non-performance while the circumstance in question subsists.[93]

Before turning to the CPWs, three preliminary points should be made. First, none of the CPWs can operate to excuse conduct which violates a peremptory norm.[94] Second, the wrongfulness of the act will only be precluded so long as the CPW continues to exist.[95] Third, the invocation of CPW is without prejudice to the question of compensation for any material loss caused by the act in question.[96]

3.5.1. Consent

If state A consents to what would otherwise be a breach of state B's obligations, the act of state B is not wrongful.[97] For example, a state might consent to transit through the airspace or internal waters of a State, the location of facilities on its territory or the conduct of official investigations or inquiries there, the exercise of jurisdiction over visiting forces, humanitarian relief and rescue operation, the arrest or detention of someone on foreign territory.[98] In each case, the consent would preclude the wrongfulness of the act. However, State A's consent is not unlimited: it cannot consent to the violation of peremptory norms of international law, such as the prohibition of genocide.[99]

3.5.2. Self-defence

A state may disregard its obligations while exercising the right of self-defence under the UN Charter,[100] Article 51 of which preserves a State's 'inherent right' of self-defence in the circumstances of an armed attack. However, the right of self-defence does not entail a blank cheque for the acting state to do as it pleases. For example, its actions are limited by principles relating to human rights and humanitarian law.[101] Moreover, the ICJ noted in its advisory opinion on the *Legality of the Threat or Use of Nuclear Weapons* that 'respect for the environment is one of

[91] Crawford and Olleson, n 41, 463.
[92] Crawford and Olleson, n 41, 465.
[93] International Law Commission, n 39, 71.
[94] International Law Commission, n 39, 26.
[95] International Law Commission, n 39, Article 27(b).
[96] International Law Commission, n 39, Article 27.
[97] International Law Commission, n 39, Article 20.
[98] International Law Commission, n 39, 72-73.
[99] International Law Commission, n 39, Article 26.
[100] International Law Commission, n 39, Article 21.
[101] International Law Commission, n 39, 74.

the elements that go to assessing whether an action is in conformity with the principles of necessity and proportionality' and thus in accordance with the right to self-defence.[102]

3.5.3. Countermeasures

Article 22 provide that the wrongfulness of an act is precluded if that act constitutes a countermeasure. Countermeasures generally refer to reprisals not involving the use of force. They may take the form of suspension or temporary non-performance of a treaty obligation, or the freezing of the assets of a state.[103] As the ICJ affirmed in the *Gabcikovo-Nagymaros Project* case, countermeasures taken by a State in response to an internationally wrongful act of another State are not wrongful acts, but are recognized as a valid means of self-help as long as certain conditions are respected.[104] Countermeasures may only be applied in limited circumstances:

'In order to be justifiable, a countermeasure must meet certain conditions . . . In the first place it must be taken in response to a previous international wrongful act of another state and must be directed against that state . . . Secondly, the injured state must have called upon the state committing the wrongful act to discontinue its wrongful conduct or to make reparation for it . . . In the view of the Court, an important consideration is that the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question . . . [and] its purpose must be to induce the wrongdoing state to comply with its obligations under international law, and . . . the measure must therefore be reversible.'[105]

The nature and scope of countermeasures are further constrained by the requirement to refrain from the use of force, to respect proportionality, and not to violate peremptory norms.[106] Moreover, the state invoking countermeasures cannot use the threat or use of force or severe political or economic political coercion designed to threaten the territorial integrity or political independence of the state. Countermeasures must be terminated as soon as the responsible state has complied with its obligations.[107]

3.5.4. Force majeure

Similar to many domestic legal systems,[108] international law precludes responsibility where the relevant act is due to circumstances outside the control of the acting state.[109] This justification only applies in very limited circumstances, when three elements are met: (a) the act in question must be brought about by an irresistible force or an unforeseen event; (b) which is beyond the control of the State concerned; and (c) which makes it materially impossible in the circumstances to perform the obligation.[110] The adjective 'irresistible' qualifying the word 'force' emphasizes that there must be a constraint which the State was unable to avoid or oppose by its own means. To have been 'unforeseen' the event must have been neither foreseen nor of an easily foreseeable kind. Further the 'irresistible force' or 'unforeseen event' must be causally linked to the situation of material impossibility, as indicated by the words 'due to *force majeure* ... making it materially impossible.'[111]

---

[102] International Law Commission, n 39, 75.
[103] Nigel White and Ademola Abass, 'Countermeasures and Sanctions' in Malcolm Evans, *International Law* (2003), 540.
[104] International Law Commission, n 39, 22.
[105] *Gabcikovo-Nagymaros Project (Hungary/Slovakia),* Judgment, ICJ Reports 1997, p. 7; [83]-[87].
[106] Crawford and Olleson, n 41, 464.
[107] International Law Commission, n 39, 75.
[108] Crawford and Olleson, n 41, 465.
[109] International Law Commission, n 39, Article 23.
[110] International Law Commission, n 39, 76.
[111] Shaw, n 40, 796.

The event giving rise to force majeure may be due to a natural or physical event (e.g. stress of weather which may divert State aircraft into the territory of another State, earthquakes, floods or drought) or to human intervention (e.g. loss of control over a portion of the State's territory as a result of an insurrection or devastation of an area by military operations carried out by a third State), or some combination of the two.[112]

The CPW of *force majeure* is further constrained by the fact that it is inapplicable if the force majeure is due to the conduct of the state invoking it or it assumed the risk of it occurring.[113] In addition, the threshold to trigger the justification of force majeure is very high. It does not does not include circumstances in which performance of an obligation has become more difficult, for example due to some political or economic crisis. Nor does it cover situations brought about by the default of the state concerned, even if the resulting injury itself was accidental and unintended.[114] For example, in the *Rainbow Warrior* arbitration,[115] France tried to invoked force majeure as a justification for repatriating French agents to France in breach of an agreement with New Zealand. This case involved the destruction by French agents of a Greenpeace vessel named 'Rainbow Warrior' in Auckland harbour. The UN Secretary-General was asked to mediate, and his ruling in 1986 provided that the French agents concerned would spend three years in French base in Pacific. France tried to argue that its repatriation of the agents before the three-year period had expired was justified by *force majeure* in the form of a medical emergency. However, this argument was rejected by the arbitration tribunal, which stressed that the test of the applicability of the doctrine was one of absolute and material impossibility, not that it was more difficult or burdensome. A similarly high threshold was applied by the PCIJ in the *Serbian Loans* case, in which the Court did not accept that WWI made it impossible for Serbia to repay a loan.[116]

For force majeure to apply, therefore, there must be an event that takes place without the state being able to do anything to rectify the event or avert its consequences. There had to be a constraint which the state was unable to avoid or to oppose by its own power. In other words, the conduct of the state is involuntary or at least involves no element of free choice.[117]

3.5.5. Distress

According to Article 24 ARSIWA, distress operates to excuse conduct where the author of the act 'had no other reasonable way ... of saving the author's life or the lives of other persons entrusted to the author's care.' This would cover, for example, aircraft or ships entering State territory under stress of weather or following mechanical or navigational failure.[118]

Shaw notes that the difference between distress and force majeure is that in the former, there is an element of choice.[119] In cases of distress, the violation of the obligation in question is theoretically avoidable, although absolute compliance of the State with its international obligations is not required. In other words, a State is not required to sacrifice human life or to suffer inordinate damage to its interests in order to fulfil its international obligations. However, the justification of distress does not apply is the situation of distress was because of the conduct of the sate invoking it or if the act in question is likely to create a comparable or greater peril.[120]

---

[112] International Law Commission, n 39, 77.
[113] International Law Commission, n 39, 78.
[114] International Law Commission, n 39, 76, 77.
[115] Rainbow Warrior Arbitration (New Zealand v France) (1990) 82 ILR 499; (1986) 74 ILR 256.
[116] *Serbian Loans,* Judgment No 14 (1929) PCIJ Ser A No 20.
[117] International Law Commission, n 39, 76.
[118] International Law Commission, n 39, 78, 79.
[119] International Law Commission, n 39, 78.
[120] International Law Commission, n 39, 81.

3.5.6. Necessity

Necessity operates to excuse an act which was the only means of safeguarding an essential interest of the state against grave and imminent peril provided that the essential interest of a second state or the international community is not seriously impaired by the act.[121] The invocation of a state of necessity is further precluded if (i) the obligation in question excludes the possibility of evoking necessity; or (iii) if state has contributed to the situation of necessity.[122] The plea of necessity is special in a number of respects. Unlike consent, self-defence, or countermeasures, it does not rely on the prior conduct of the injured State. Unlike *force majeure,* it does not involve conduct which is coerced or involuntary. Unlike distress, necessity applies where there is a grave danger either to the essential interests of the State or of the international community as a whole, rather than in circumstances where there is a danger to the lives of individuals in the charge of a State official. It arises where there is an incompatible conflict between an essential interest on the one hand and an obligation of the State invoking necessity on the other. These special features mean that necessity will only rarely be available to excuse non-performance of an obligation and that it is subject to strict limitations to protect against possible abuse.[123]

According to the commentaries on the Article, the claim of necessity was applicable in respect of the Torrey Canyon incident. A Liberian oil tanker went aground off the UK coast but outside territorial waters, spilling large quantities of oil and endangering the UK coastline. After salvage attempts, the UK bombed the ship to burn the remaining oil. The British Government did not advance any legal justification for its conduct, but stressed the existence of a situation of extreme danger and claimed that the decision to bomb the ship had been taken only after all other means had failed. No international protest resulted. A convention was subsequently concluded to cover future cases where intervention might prove necessary to avert serious oil pollution.[124]

4. Invocation of Responsibility

An injured state is entitled to invoke the responsibility of the state which committed an internationally wrongful act towards it.[125] However, Article 48(1) provides that a state other than the injured state are also entitled to invoke the responsibility of the acting state if (a) the obligation breached is owed to a group of states including that state and it established for the protection of a collective interest of the group (sometimes called '*erga omnes partes'*) or ; (b) the obligation breached is owed to the international community as a whole (sometimes called '*erga omnes')*.

Article 48(1)(a) may include obligations under multilateral treaties protecting 'community' interests such as obligations under human rights or environmental law. The states falling within situations covered in Article 48(1) will not normally have suffered any injury. Such states should be limited to claiming cessation of continuing wrongful acts and assurances and guarantees of non-repetition, as well as performance of the obligation of reparation 'in the interest of the injured state or the beneficiaries of the obligation breached.'[126] Obligations *erga omnes partes* were addressed by the ICJ in *Questions Relation to the Obligation to Prosecute or Extradite*, a dispute relating to the Convention Against Torture:

The common interest in compliance with the relevant obligations under the Convention against Torture implies the entitlement of each State party to the Convention to make a claim concerning

[121] International Law Commission, n 39, Article 25.
[122] Shaw, n 40, 798.
[123] International Law Commission, n 39, 81.
[124] International Law Commission, n 39, 82.
[125] International Law Commission, n 39, 42.
[126] International Law Commission, n 39, Articles 48(2)(a) and (b).

the cessation of the alleged breach by another State party. If a special interest were required for that purposes, in many cases no Stat would be in the position to make such a claim. It follows that any State party to the Convention may invoke the responsibility of another State party with a view to ascertaining the alleged failure to comply with its obligations erga omnes partes […] and to bring that failure to an end.[127]

Article 48(1)(b) encompasses the concept of *erga omnes*, which refers to obligations owed to the international community as a whole. These 'are the concern of all States. In the view of the importance of the rights involved, all States can be held to have a legal interest in their protection.'[128] Such obligations might include the acts of aggression and genocide, 'the principles and rules concerning the basic rights of the human person, including protection from slavery and discrimination', the right of self-determination, obligations of international humanitarian law which form 'intransgressible principles of customary international law' as well as the prohibition of torture.[129]

5. The Consequences of International Responsibility

Upon the commission of an internationally wrongful act, two main secondary obligations arise: the obligations of cessation and reparation.[130] These dual obligations arise because state responsibility is both backward-looking (aimed at providing compensation for things past) and forward-looking (aimed at restoring the legal relationship which has been threatened or impaired by the breach).[131]

The obligation to cease wrongful conduct also incorporates an obligation, under certain circumstances, to offer appropriate assurances and guarantees of non-repetition. This issue was dealt with in the *LaGrand* case before the ICJ, which concerned the USA's non-observance of obligations of consular notification under Article 36 of the Vienna Convention on Consular Relations. Germany complained that the US had failed to notify it that two German nationals were death-row inmates, and there was a broader concern as to the USA's compliance with its continuing obligations of performance under the Consular Relations Convention. The USA accepted this contention, and set out the measures it had taken to ensure compliance for the future. The Court held:

[That the commitment expressed by the United States to ensure implementation of the specific measures adopted in performance of its obligations under Article 36, paragraph 1(b), must be regarded as meeting Germany's request for a general assurance of non-repetition.[132]

As aforementioned, the obligation of reparation also arises where actual harm or damage has occurred. International law obliges the responsible state to make full reparation for the consequences of its breach, provided it is not too remote or indirect. As noted in the *Chorzow*

Factory case:

The essential principle contained in the actual notion of an illegal act – a principle which seems to be established by international practice and by the decisions of arbitral tribunals – is that reparation must, so far as possible, wipe out all the consequences of the illegal act and re-establish

[127] Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal), Judgment, ICJ Reports 2012, p. 422 [69].

[128] Barcelona Traction, Light and Power Company, Limited, Second Phase, Judgment, ICJ Reports 1970, p. 3 [33].

[129] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996, p. 226 [79].

[130] Crawford and Olleson, n 41, 465.

[131] Crawford and Olleson, n 41.

[132] LaGrand (Germany v United States of America), Merits, judgment, (2001)40 1LM 1069, [24].

the situation which would, in all probability, have existed if that act had not been committed. Restitution in kind, or if this this is not possible, payment of a sum corresponding to the value which a restitution in kind would bear; the award, if need be, of damages for loss sustained which would not be covered by restitution in kind or payment in place of it – such are the principles which should serve to determine the amount of compensation due for an act contrary to international law.[133]

Reparation may be in forms other than compensation, such as an acknowledgment of the breach, an expression of regret, an apology, or other appropriate form.[134] In many cases before international courts, an authoritative finding of the breach may be held to be sufficient satisfaction.[135]

6. State Responsibility and Cybersecurity

General principles of state responsibility apply also in the cybersecurity context. However, the application of the state responsibility paradigm to cybersecurity attacks is complicated by several factors.

First, it is often difficult to identify an international obligation that has been breached.[136] The law of cyberspace is still a relatively nascent field that has not been codified[137] and where customary law has not emerged yet. Therefore, it is necessary to resort to principles of general international law. Three typical international obligations that are particularly relevant in the cybersecurity context are respect for the target State sovereignty, the duty of non-intervention in the internal or external affairs of the target State, and the principle of due diligence.[138]

However, the application of each of these three principles faces numerous challenges in the cybersecurity context. In order to invoke the violation of State sovereignty, it is necessary to prove the infringement of a target State's territorial integrity or the interference with or usurpation of inherently governmental functions.[139] This might be doable when cyber operations result in "physical damage or injury" or the "loss of functionality" of cyber infrastructure in the target State.[140] But the application of these requirements to the cyber influence operations such as election meddling or cyberespionage will be far more challenging.[141] Similarly, the intervention is unlawful only if it meets two cumulative conditions– if it "bear[s] on matters in which each State is permitted, by the principle of State sovereignty to decide freely"[142] and "when it uses methods

---

[133] *Factory at Chorzow*, Merits, 1928, PCIJ, Series A, No 17, p. 27, pp. 47-48.

[134] Crawford and Olleson, n 41, 467.

[135] Crawford and Olleson, n 41, 468; *Corfu Channel, Merits, Judgment, I.C.J. Reports 1949*, p. 4, at p. 23.

[136] See Barrie Sander, Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections, *Chinese Journal of International Law*, Volume 18, Issue 1, March 2019, 1, at 17-26.

[137] But see the Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017) (hereinafter only 'Tallinn Manual 2.0'). See also Dan Efrony and Yuval Shany, A Rule Book on The Shelf? Tallinn 2.0 on Cyber Operations and Subsequent State Practice, 112 American Journal of International Law (2018).

[138] Barrie Sander, Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections, *Chinese Journal of International Law*, Volume 18, Issue 1, March 2019, 1, at 17-26.

[139] Tallinn Manual 2.0, 20.

[140] Tallinn Manual 2.0, 20-21.

[141] Tallinn Manual 2.0, 21-22. See also Jens D. Ohlin, Did Russian Cyber Interference in the 2016 Election Violate International Law, 95 Texas Law Review (2017), 1588 and 1593-1594; Michael N. Schmitt, "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law, 19 Chicago Journal of International Law, 39-42; and Ido Kilovaty, Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information, 9 Harvard National Security Journal (2018).

[142] Military and Paramilitary Activities in and against Nicaragua, Merits, Judgment (Nicaragua v United States of America), ICJ Reports 1986, p. 14, [205].

of coercion".[143] That is again challenging in the cybersecurity context as the boundaries of the *domaine reservé* have been vague and the coercion has traditionally been understood narrowly in kinetic conflicts.[144] Finally, claiming the breach of the duty of due diligence faces even greater challenges as the status of the principle of due diligence in contested both in the general international law[145] as well as in the cyber context[146] and the scope of this principle is unclear.[147]

Second, even if the international norm breached by a cyber operation has been identified, it is not always easy to attribute this international wrongful act to a State.[148] In fact, the attribution of cyber operations to a State faces not only legal but also technical and political challenges.[149] In order to satisfy the attribution requirements, it is necessary to identify both "location and identity of the cyber infrastructure from which an operation originates ("technical attribution")"[150] and "the person who was operating the infrastructure("political attribution")".[151] This tracing is still slow and cumbersome. But even if this is done, it is still necessary to prove a sufficient link between a breach of international law and a State ("legal attribution"). Given the fact that cyberoperations can be easily outsourced to non-State actors, this element presents a daunting challenge.[152]

Finally, it is also important to bear in mind the contextual factors. Cybertechnology has been advancing quickly and international law has been somewhat lagging behind,[153] partly also due to the private internet governance.[154] At the same time, the States have been creative in employing cyber tools to advance their interests. The cyber-attacks thus do not entail only attacks on infrastructure, but also election meddling, cyberespionage and other influence operations that are difficult to classify under the standard state responsibility paradigm. The rise of artificial

---

[143] Military and Paramilitary Activities in and against Nicaragua, Merits, Judgment (Nicaragua v United States of America), ICJ Reports 1986, p. 14, [205].

[144] See Tallinn Manual 2.0, 315-319; and Robert Jennings and Arthur Watts (eds.), Oppenheim's International Law (9th ed., 2008), 432. But see the recent works that argue for a broader understanding of coercion, in particular Michael N. Schmitt, Grey Zones in the International Law of Cyberspace, 42 Yale Journal of International Law (2017); Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage, in: Anna-Maria Osula and Henry Rogias (eds.), International Cyber Norms: Legal, Policy & Industry Perspectives (2016), 78; and Sean Watts, Low-Intensity Cyber Operations and the Principle of Non-Intervention, in Jens D. Ohlin et al. (eds.), Cyber War: Law and Ethics for Virtual Conflicts (2015), 257

[145] See e.g. McDonald, N. (2019). The Role of Due Diligence In International Law. *International and Comparative Law Quarterly, 68*(4), 1041-1054.

[146] See Barrie Sander, Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections, *Chinese Journal of International Law*, Volume 18, Issue 1, March 2019, 1, at 24.

[147] See Barrie Sander, Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections, *Chinese Journal of International Law*, Volume 18, Issue 1, March 2019, 1, at 25-26.

[148] See Barrie Sander, Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections, *Chinese Journal of International Law*, Volume 18, Issue 1, March 2019, 1, at 26-28.

[149] Nicholas Tsagourias, Cyber Attacks, Self-Defence and the Problem of Attribution, 17 Journal of Conflict & Security Law (2012).

[150] Barrie Sander, Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections, *Chinese Journal of International Law*, Volume 18, Issue 1, March 2019, 1, at 26.

[151] Ibid (citation omitted).

[152] See Barrie Sander, Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections, *Chinese Journal of International Law*, Volume 18, Issue 1, March 2019, 1, at 27-28.

[153] See Eyal Benvenisti, 'Upholding DemocracyAmid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29(1) European Journal of International Law 9.

[154] See Menashe, M., & Kikarea, E. (2019). The global governance of cyberspace: reimagining private actors' accountability: introduction. Cambridge International Law Journal, 8 (2), 153-170. See also Roxana Radu, *Negotiating Internet Governance*, OUP, 2019.

intelligence will make this even more complicated. We thus need to "think infrastructally"[155] and carefully watch the emerging State practice in this vibrant area of international law.

7. Conclusion

Every internationally wrongful act by a subject of international law entails its international responsibility.[156] The ILC has done an admirable job in clarifying how this overarching principle of state responsibility operates in terms of attribution, breach of an obligation, circumstances precluding wrongfulness, as well as the invocation and consequences of state responsibility. International and domestic case law has laid the foundation for and - in some cases - progressively developed these rules. However, state responsibility remains an amorphous area of law as is illustrated by its application to the cybersecurity context. The rapid development of cybertechnology, the corresponding underdevelopment of cybersecurity law, as well as the difficulty in identifying where there has been a violation of state sovereignty and/or attribution of the respective act to the state all pose challenges when applying the rules of state responsibility in the cybersecurity sphere.

[155] Benedict Kingsbury, Infrastructure and InfraReg: on rousing the international law 'Wizards of Is', Cambridge International Law Journal, Vol. 8 No. 2, pp. 171–186.

[156] See the dictum of the *Permanent Court of International Justice in Factory at Chorzow, jurisdiction, judgment No B, 1927, PClj, Ser A, No 9* at p 21: 'It is a principle of international law that the breach of an engagement involves an obligation to make reparation'.

Use of Force

Ivana Kudláčková, Kateřina Uhlířová

The use of force in international law and the use of international law in cyberspace

1. The use of force in international law

The rules governing the use of force form 'a central element' in public international law,[157] and, coupled with principles such as the independence and equality of states and territorial sovereignty, provide 'the framework for international order.'[158] These rules are to be found in customary international law and the United Nations Charter[159] (Charter). The Charter contains a prohibition of the threat or use of force (Article 2 paragraph 4)[160] as well as the provisions referring to two circumstances in which this prohibition does not apply.[161] First, the United Nations Security Council can take or authorize enforcement measures including the use of (armed) force under Chapter VII of the Charter. Second, Article 51 of the Charter provides for the right of individual or collective self-defense. While rules governing the use of force are 'relatively easy to state', they often prove 'difficult to apply in practice.'[162]

2. The use of international law in cyberspace

Transposed to our 'cyberspace' scenario, the picture is further complicated by the on-going debate about the extent to which international law applies in cyberspace and, in particular, whether cyber operations[163] may constitute use of force within the meaning of Article 2 paragraph 4 of the Charter and customary international law.[164] As such, this topic includes cutting-edge issues of international law relating to the application of rules governing the use of force (*jus ad bellum*) as

---

[157] Malcolm Shaw, *International Law*, CUP, 2008, p. 118.
[158] Ibid. See also Marc Weller (ed.), The Oxford Handbook of the Use of Force in International Law, OPU, 2015. Yoram Dinstein, War, Aggression and Self-Defense, CUP, 2017. Christine Gray, International Law and the Use of Force, OUP, 2018.
[159] Michael Wood, International Law and the Use of Force: What Happens in Practice? *Indian Journal of International Law*, Volume 53, 2013, p. 351.
[160] Compare with: 'All members of the Organization shall refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of the Organization.' In Dumbarton Oaks Proposal for the Establishment of a General International Organization, UNCIO Vol. III, 1 [online]. 1945.
[161] Michael Wood, International Law and the Use of Force: What Happens in Practice? *Indian Journal of International Law*, Volume 53, 2013, p. 351.
[162] Ibid.
[163] For (one of) the definitions of cyber operations, see e.g. the Joint Chiefs of Staff, U.S. Department of Defense, Joint Publications Operations Series, available at https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/. According to the Joint Chiefs of Staff, cyber operations include, but are not limited to, computer network attack, computer network defense, and computer network exploitation. See also Marco Roscini: 'Even though the most extreme scenarios have not occurred yet, a cyber operation could go as far as to disable power generators, cut off the military command, control, and communication systems, cause trains to derail and aeroplanes to crash, nuclear reactors to melt down, pipelines to explode, weapons to malfunction, banking systems to cripple'. Marco Roscini, *Cyber operations and the use of force in international law*. OUP, 2014, p. 2.
[164] Harold Hongju Koh, International Law in Cyberspace, *Harvard International Law Journal*, Volume 54, December 2012, p. 3.

well as the body of international law that regulates behaviour during armed conflict (*jus in bello*). The focus of this chapter is predominantly on the rules of *jus ad bellum*. In a nutshell, we suggest that (i) established principles of international law do apply in cyberspace[165], (ii) cyber activities may in certain—highly specific—circumstances constitute a use of force[166] and finally, (iii) a state may respond to cyber activities which amount to an armed attack by exercising a right of self-defense.[167] That said, cyber activities clearly open up 'a host of novel and extremely difficult legal issues'[168] and bring a number of unresolved questions such as the following: How can the 'old' rules of *jus ad bellum* take into account all of the 'new' kinds of effects possibly produced by states 'through the click of a button'?[169] How do we address 'dual-use infrastructure' and how do we approach the problem of attribution in cyberspace?[170] When grappling with all these and many

---

[165] See e.g. a statement by Marina Kaljurand, (then) adviser to the Estonian Ministry of Foreign Affairs in matters of security and Estonia's representative on the UN's Group of Governmental Experts on Cybersecurity: 'The international community has agreed that international law applies to cyberspace. But the big question is how, because when international law developed we didn't have any idea of cyberspace.' In Dario Cavegn, Marina Kaljurand: The Essence of the Tallinn Manual, *ERR News*, 17 February 2017, available at https://news.err.ee/121053/marina-kaljurand-the-essence-of-the-tallinn-manual.

[166] See e.g. Harold Hongju Koh arguing that 'cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example, (1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction, or (3) operations that disable air traffic control resulting in airplane crashes.' Harold Hongju Koh, International Law in Cyberspace, *Harvard International Law Journal*, Volume 54, December 2012, p. 3. See also Michael N. Schmitt, The Law of Cyber Warfare: Quo Vadis? *Stanford Law and Policy Review*, Volume 25, Issue 2, 2014, p. 280, Kateřina Uhlířová, Zásada zákazu použití síly a „počítačový útok" proti kritickým infrastrukturám státu: vacuum iuris či výkladová výzva? In Tereza Kyselovská, David Sehnálek, Naděžda Rozehnalová (eds.), *In Varietate Concordia: soubor vědeckých statí k poctě prof. Vladimíra Týče*, Masarykova univerzita, 2019, pp. 413-464.

[167] See e.g. the US Declaratory Policy for Cyber Deterrence, The White House, International Strategy for Cyberspace, May 2011, '[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners', available at https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. See also statement by (then) Secretary of State, Hillary Clinton, suggesting that attacks on allied cyber and energy infrastructures should be considered as attacks under Article 5 of the North Atlantic Treaty, further declaring that 'in the 21st century, the spirit of collective defense must also include non-traditional threats'. In James Joyner, Cyber Attacks and Article 5, *Atlantic Council*, 2 July 2010, available at https://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-and-article-5/. See also Marina Kaljurand, (then) adviser to the Estonian Ministry of Foreign Affairs in matters of security: 'In 2007 there also was the question whether or not to trigger NATO Article 4 or 5. But the answer was very simple, those attacks were not destructive, they didn't kill anybody, they just interfered with our e-lifestyle. And as we were looking at the effects, we decided to retaliate in the way we did.' In Dario Cavegn, Marina Kaljurand: The Essence of the Tallinn Manual, *ERR News*, 17 February 2017, available at https://news.err.ee/121053/marina-kaljurand-the-essence-of-the-tallinn-manual.

[168] Harold Hongju Koh, International Law in Cyberspace, *Harvard International Law Journal*, Volume 54, December 2012, p. 3.

[169] Ibid., p. 7.

[170] Ibid., p. 8. For legal challenges connected with the problem of attribution, see e.g. the malicious cyber operations that accompanied the actual military attacks in Georgia or Ukraine, or cyber attack in Estonia: 'First, we gathered evidence, asked for clarification from Russia, and then we took countermeasures. We put individuals behind the cyberattacks on the so-called Schengen blacklist. Compare this with what the United States did after the DNC incident, they expelled diplomats. So today we can say that we have already some practice applying international law. We have examples how countries can react to cyber operations'. In Dario Cavegn, Marina Kaljurand: The Essence of the Tallinn Manual, *ERR News*, 17 February 2017,

more questions, it is crucial to stay 'faithful to enduring principles, while accounting for changing times and technologies'.[171] Against this background, we offer below a plethora of sources that may help to elucidate the complexity and contemporary challenges of how international law applies in cyberspace, especially in the context of the prohibition of threat or use of force. These materials range from hard law to soft law, from case law of international courts and tribunals[172] to practice of international organizations.

3. Charter of the United Nations, 26 June 1945

Article 2

The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

(…)

4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Article 39

The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

Article 41

The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

Article 42

Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as

---

available at https://news.err.ee/121053/marina-kaljurand-the-essence-of-the-tallinn-manual. See also Ali Akbar Salehi, Minister of Foreign Affairs of the Islamic Republic of Iran: 'As a country that not only whose nationals have been targeted by terrorist groups, but also its nuclear facilities have been subject to cyber attacks […].' In Statement by Ali Akbar Salehi, Minister of Foreign Affairs of the Islamic Republic of Iran, At the High Level Meeting on Countering Nuclear Terrorism [online], United Nations, New York, 28 September 2012.

[171] Harold Hongju Koh, International Law in Cyberspace, *Harvard International Law Journal*, Volume 54, December 2012, p. 2.

[172] For the role of international case law in the domestic law, see Kateřina Uhlířová, War Crimes Chamber of the Court of Bosnia and Herzegovina: Seeding "International Standards of Justice"? In Edda Kristjánsdóttir, André Nollkaemper, Cedric Ryngaert (eds.), *International Law in Domestic Courts: Rule of Law Reform in Post-Conflict States*, Series on Transitional Justice, Cambridge: Intersentia, 2012, pp. 195-217.

may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

Article 51

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

4. The North Atlantic Treaty, Washington D.C., 4 April 1949

Article 5

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

5. The Draft Articles on Responsibility of States for Internationally Wrongful Acts, The International Law Commission, UN Doc A/56/10

Article 1. Responsibility of a State for its internationally wrongful acts

Every internationally wrongful act of a State entails the international responsibility of that State.

Article 2. Elements of an internationally wrongful act of a State

There is an internationally wrongful act of a State when conduct consisting of an action or omission:

(a) is attributable to the State under international law; and

(b) constitutes a breach of an international obligation of the State.

Article 4. Conduct of organs of a State

1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its char- acter as an organ of the central Government or of a territorial unit of the State.

2. An organ includes any person or entity which has that status in accordance with the internal law of the State.

Article 5. Conduct of persons or entities exercising elements of governmental authority

The conduct of a person or entity which is not an organ of the State under article but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance.

Article 7. Excess of authority or contravention of instructions

The conduct of an organ of a State or of a person or entity empowered to exercise elements of the governmental authority shall be considered an act of the State under international law if the organ, person or entity acts in that capacity, even if it exceeds its authority or contravenes instructions.

Article 8. Conduckt directed or controlled by a State

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

(1)As a general principle, the conduct of private persons or entities is not attributable to the State under international law. Circumstances may arise, however, where such conduct is nevertheless attributable to the State because there exists a specific factual relationship between the person or entity engaging in the conduct and the State. Article 8 deals with two such circumstances. The first involves private persons acting on the instructions of the State in carrying out the wrongful conduct. The second deals with a more general situation where private persons act under the State's direction or control.153 Bearing in mind the important role played by the principle of effectiveness in international law, it is necessary to take into account in both cases the existence of a real link between the person or group performing the act and the State machinery.

(3) More complex issues arise in determining whether conduct was carried out "under the direction or control" of a State. Such conduct will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation. The principle does not extend to conduct which was only incidentally or peripherally associated with an operation and which escaped from the State's direction or control.

(4) The degree of control which must be exercised by the State in order for the conduct to be attributable to it was a key issue in the *Military and Paramilitary Activities in and against Nicaragua* case. The question was whether the conduct of the contras was attributable to the United States so as to hold the latter generally responsible for breaches of international humanitarian law committed by the contras. This was analysed by ICJ in terms of the notion of "control". On the one hand, it held that the United States was responsible for the "planning, direction and support" given by the United States to Nicaraguan operatives. But it rejected the broader claim of Nicaragua that all the conduct of the contras was attributable to the United States by reason of its control over them.

(5) The Appeals Chamber of the International Tribunal for the Former Yugoslavia has also addressed these issues. In the Tadić, case, the Chamber stressed that:

The requirement of international law for the attribution to States of acts performed by private individuals is that the State exercises control over the individuals. The degree of control may, however, vary according to the factual circumstances of each case. The Appeals Chamber fails to see why in each and every circumstance international law should require a high threshold for the test of control.

Article 11. Conduct acknowledged and adopted by a State as its own

Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.

(4) Outside the context of State succession, the United States Diplomatic and Consular Staff in Tehran case provides a further example of subsequent adoption by a State of particular conduct. There ICJ drew a clear distinction between the legal situation immediately following the seizure of the United States embassy and its personnel by the militants, and that created by a decree of the Iranian State which expressly approved and maintained the situation.

6. Tallinn Manual on The International Law Applicable to Cyber Warfare

Rule 1 – Sovereignty

7. If such cyber operations are intended to coerce the government (and not otherwise permitted under international law), the operation may constitute a prohibited 'intervention'24 or a prohibited 'use of force' (Rules 10 to 12). A cyber operation that qualifies as an 'armed attack' triggers the right of individual or collective self-defence (Rule 13). Actions not constituting an armed attack but that are nevertheless in violation of international law may entitle the target State to resort to countermeasures (Rule 9). Security Council-mandated or authorized actions under Chapter VII of the United Nations Charter (Rule 18), including those involving cyber operations, do not constitute a violation of the target State's sovereignty.

Rule 10 – Prohibition of Threat or Use of Force

A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.

1. Article 2(4) of the United Nations Charter provides that "All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations". The prohibition is undoubtedly a norm of customary international law.95

2. In addition to the specific prohibition of threats or uses of force against the territorial integrity or political independence of any State, the United Nations Charter's travaux préparatoires suggest that the reference in Article 2(4) to threats or uses of force inconsistent with the "purposes of the United Nations" (laid down in Article 1 of the Charter) was intended to create a presumption of illegality for any threat or use of force.96 In other words, even acts that are not directed against either the territorial integrity or political independence of a State may nevertheless violate the prohibition if they are inconsistent with the purposes of the United Nations. There are two widely acknowledged exceptions to the prohibition on the use of force — uses of force authorized by the Security Council under Chapter VII (Rule 18) and self-defence pursuant to Article 51 and customary international law (Rule 13). The International Group of Experts did not take a position as to the lawfulness of other uses of force, such as humanitarian intervention.

3. The terms 'use of force' and 'threat of the use of force' are defined in Rules 11 and 12 respectively.

4. An action qualifying as a 'use of force' need not necessarily be undertaken by a State's armed forces. For example, it is clear that a cyber operation that would qualify as a 'use of force' if

conducted by the armed forces would equally be a 'use of force' if undertaken by a State's intelligence agencies or by a private contractor whose conduct is attributable to the State based upon the law of State responsibility. With regard to those entities whose actions may be attributed to States, see Rules 6-8.

5. Although, by its own express terms, Article 2(4) applies solely to Members of the United Nations, the prohibition also extends to non-member States by virtue of customary international law. However, Article 2(4) and its customary international law counterpart do not apply to the acts of non-State actors, including individuals, organized groups, and terrorist organizations, unless they are attributable to a State pursuant to the law of State responsibility (Rule 6). In such a case, it would be the State, not the non- State actor, which is deemed to be in violation. The actions of non-State actors may be unlawful under international and domestic law, but not as a violation of the prohibition on the use of force.

6. The fact that a cyber operation does not rise to the level of a use of force does not necessarily render it lawful under international law. In particular, a cyber operation may constitute a violation of the prohibition on intervention. Although not expressly set out in the United Nations Charter, the prohibition of intervention is implicit in the principle of the sovereign equality of States laid out in Article 2(1) of the United Nations Charter. It is mentioned in a number of treaties and United Nations resolutions, the most significant of which is the Declaration on Friendly Relations.. According to the International Court of Justice, the principle is "part and parcel of customary international law".97

7. The precise scope and content of the non-intervention principle remains the subject of some debate. In the Nicaragua case, the International Court of Justice held that "the principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States".98 Therefore, "a prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy."99 For instance, the Court held that supplying funds to insurgents was "undoubtedly an act of intervention in the internal affairs of Nicaragua", although not a use of force.100

Rule 11 – Definition of Use of Force

A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.

1. This Rule examines the term 'use of force' found in Rule 10. The United Nations Charter offers no criteria by which to determine when an act amounts to a use of force. In discussions regarding the appropriate threshold for a use of force, the International Group of Experts took notice of the Nicaragua Judgment. In that case, the International Court of Justice stated that 'scale and effects' are to be considered when determining whether particular actions amount to an 'armed attack' (Rule 13).103 The Experts found the focus on scale and effects to be an equally useful approach when distinguishing acts that qualify as uses of force from those that do not. In other words, 'scale and effects' is a shorthand term that captures the quantitative and qualitative factors to be analysed in determining whether a cyber operation qualifies as a use of force.

2. There is no authoritative definition of, or criteria for, 'threat' or 'use of force'. However, certain categories of coercive operations are not uses of force. At the 1945 Charter drafting conference in San Francisco, States considered and rejected a proposal to include economic coercion as a use of force.104 The issue arose again a quarter of a century later during the proceedings leading to the General Assembly's Declaration on Friendly Relations. The question of whether 'force' included "all forms of pressure, including those of a political or economic character, which have the effect of threatening the territorial integrity or political independence of any State" was answered in the negative.105 Accordingly, whatever 'force' may be, it is not mere economic or political coercion.

Cyber operations that involve, or are otherwise analogous to, these coercive activities are definitely not prohibited uses of force.

3. As an example, non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy do not qualify as uses of force. Additionally, the International Court of Justice held in the Nicaragua case that merely funding guerrillas engaged in operations against another State did not reach the use of force threshold.106 Thus, for instance, merely funding a hacktivist group conducting cyber operations as part of an insurgency would not be a use of force.

4. A use of force need not involve the employment of military or other armed forces by the State in question. In Nicaragua, the International Court of Justice found that arming and training a guerrilla force that is engaged in hostilities against another State qualified as a use of force.107 Therefore, providing an organized group with malware and the training necessary to use it to carry out cyber attacks against another State would also qualify.

5. This conclusion raises the question of whether affording sanctuary (safe haven) to those mounting cyber operations of the requisite severity amounts to a 'use of force' (or 'armed attack').108 The majority of the International Group of Experts took the position that in most cases simply granting sanctuary is insufficient to attribute the actions of non- State actors to the State for the purpose of finding a use of force by that State. Similarly, they did not deem the failure of a State to police its territory in order to prevent the launch of cyber operations to be a use of force (but see Rule 5 on the obligations of States vis-à-vis control over cyber infrastructure). That said, the majority agreed that the provision of sanctuary coupled with other acts, such as substantial support or providing cyber defences for the non-State group, could, in certain circumstances, be a use of force.

6. In determining whether an act constitutes a 'use of force', it is useful to consider the notion of 'armed attack', which is the threshold at which a State may lawfully use force in self-defence (Rule 13). In the Nicaragua Judgment, the International Court of Justice distinguished the "most grave" forms of the 'use of force' (those constituting an 'armed attack' for the purposes of the law of self-defence) from other less grave forms.109 The International Group of Experts agreed, therefore, that any cyber operation which rises to the level of an 'armed attack' in terms of scale and effects pursuant to Rule 13, and which is conducted by or otherwise attributable to a State, qualifies as a 'use of force'.

7. The International Group of Experts acknowledged a contrary view whereby the distinction between the two concepts is either so narrow as to be insignificant or non- existent. This position, articulated by the United States after the Nicaragua decision, asserts that any illegal use of force can qualify as an armed attack triggering the right of self-defence; there is no gravity threshold distinguishing illegal uses of force from armed attacks.110 On this view, no gap exists between an unlawful use of force and an armed attack, although the principles of necessity and proportionality that apply to actions in self-defence may limit the responses available to a State that has been attacked.

8. To summarize, some cyber actions are undeniably not uses of force, uses of force need not involve a State's direct use of armed force, and all armed attacks are uses of force. This leaves unresolved the question as to what actions short of an armed attack constitute a use of force. Acts that injure or kill persons or damage or destroy objects are unambiguously uses of force (see Commentary to Rule 13 expressing an analogous conclusion, but requiring the harm to be 'significant'). Since other cases are less clear, the International Group of Experts took notice of an approach that seeks to assess the likelihood that States will characterise a cyber operation as a use of force.111 The method expounded operates on the premise that in the absence of a conclusive definitional threshold, States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition on the use of force.

9. The approach focuses on both the level of harm inflicted and certain qualitative elements of a particular cyber operation. In great part, the approach is intended to identify cyber operations that are analogous to other non-kinetic or kinetic actions that the international community would describe as uses of force. To the extent such operations would be assessed as reaching the use of force threshold, so too would cyber operations of the same scale and effects. The approach suggests that States are likely to consider and place great weight on the following factors, inter alia, when deciding whether to characterise any operation, including a cyber operation, as a use of force. It must be emphasized that they are merely factors that influence States making use of force assessments; they are not formal legal criteria.

(a) Severity: Subject to a de minimis rule, consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force. Those generating mere inconvenience or irritation will never do so. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scope, duration, and intensity of the consequences will have great bearing on the appraisal of their severity. A cyber operation, like any operation, resulting in damage, destruction, injury, or death is highly likely to be considered a use of force. Severity is self-evidently the most significant factor in the analysis.

(b) Immediacy: The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, States harbour a greater concern about immediate consequences than those that are delayed or build slowly over time, and are more likely to characterize a cyber operation that produces immediate results as a use of force than cyber actions that take weeks or months to achieve their intended effects.

(c) Directness: The greater the attenuation between the initial act and its consequences, the less likely States will be to deem the actor in violation of the prohibition on the use of force. Whereas the immediacy factor focuses on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, market forces, access to markets, and the like determine the eventual consequences of economic coercion (e.g., economic downturn). The causal connection between the initial acts and their effects tends to be indirect—economic sanctions may take weeks or even months to have a significant effect. In armed actions, by contrast, cause and effect are closely related. An explosion, for example, directly harms people or objects. Cyber operations in which the cause and effect are clearly linked are more likely to be characterised as uses of force.

(d) Invasiveness: Invasiveness refers to the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State. As a rule, the more secure a targeted cyber system, the greater the concern as to its penetration. For example, intrusion into a military system that has been accredited at Evaluation Assurance Level 7 (EAL7) of the Common Criteria is more invasive than merely exploiting vulnerabilities of an openly accessible non-accredited system at a civilian university or small business.112 Additionally, the degree to which the intended effects of a cyber operation are limited to a particular State increases the perceived invasiveness of those operations.

Domain name is a highly visible indicator in cyberspace and for that reason may carry significance in assessing the extent of invasiveness of an operation. Cyber operations that specifically target the domain name of a particular State (e.g., 'mil.ee') or of a particular State organ may, for this reason, be considered more invasive than those operations directed at non-State specific domain name extensions such as '.com'. This factor must be cautiously applied in the cyber context. In particular, computer network exploitation is a pervasive tool of modern espionage. Though highly invasive, cyber espionage does not rise to the level of a use of force due to the absence of a direct prohibition in international law on espionage per se (Rule 66). Thus, actions such as disabling cyber security mechanisms in order to monitor (e) Measurability of effects: This factor derives from the greater willingness of States to characterize actions as a use of force when the

consequences are apparent. Traditionally, the armed forces carried out operations that qualified as uses of force and the effects of the operations were generally measurable (as in the case of battle damage assessments). In the cyber realm, consequences may be less apparent. Therefore, the more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of a use of force. Accordingly, a cyber operation that can be evaluated in very specific terms (e.g., amount of data corrupted, percentage of servers disabled, number of confidential files exfiltrated) is more likely to be characterized as a use of force than one with difficult to measure or subjective consequences.

(f) Military Character: A nexus between the cyber operation in question and military operations heightens the likelihood of characterization as a use of force. This contention is supported by the fact that the United Nations Charter is particularly concerned with military actions. Its preamble provides that "armed force shall not be used, save in the common interest",113 while Article 44 uses the term 'force' without the qualifier 'armed' in a situation that clearly refers to the use of military force. Further, the use of force has traditionally been understood to imply force employed by the military or other armed forces.

(g) State involvement: The extent of State involvement in a cyber operation lies along a continuum from operations conducted by a State itself (e.g., the activities of its armed forces or intelligence agencies) to those in which its involvement is peripheral. The clearer and closer a nexus between a State and cyber operations, the more likely it is that other States will characterize them as uses of force by that State.114

(h) Presumptive legality. International law is generally prohibitive in nature.115 Acts that are not forbidden are permitted; absent an express treaty or accepted customary law prohibition, an act is presumptively legal. For instance, international law does not prohibit propaganda, psychological operations, espionage, or mere economic pressure per se. Therefore, acts falling into these and other such categories are presumptively legal (although in a particular situation they may in fact violate an international law norm). This being so, they are less likely to be considered by States as uses of force.

10. These factors are not exhaustive. Depending on the attendant circumstances, States may look to others, such as the prevailing political environment, whether the operation portends the future use of military force, the identity of the attacker, any record of cyber operations by the attacker, and the nature of the target (such as critical infrastructure). Moreover, the factors operate in concert. As an example, a highly invasive operation that causes only inconvenience such as temporary denial of service is unlikely to be classified as a use of force. By contrast, some may categorize massive cyber operations that cripple an economy as a use of force even though economic coercion is presumptively lawful.

11. Finally, it must be understood that 'use of force' as used in this Rule and 'armed attack' (Rule 13) are standards that serve different normative purposes. The 'use of force' standard is employed to determine whether a State has violated Article 2(4) of the United Nations Charter and the related customary international law prohibition. By contrast, the notion of 'armed attack' has to do with whether the target State may respond to an act with a use of force without itself violating the prohibition on using force. This distinction is critical in that the mere fact that a use of force has occurred does not alone justify a use of force in response.116 States facing a use of force not amounting to an armed attack will, in the view of the International Group of Experts, have to resort to other measures if it wishes to respond lawfully, such as countermeasures (Rule 9) or actions consistent with the plea of necessity (Commentary accompanying Rule 9).

Rule 12 – Definition of Threat of Force

A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force.

1. This Rule examines the term 'threat' as used in Rule 10.

2. The phrase 'cyber operation, or threatened cyber operation' in this Rule applies to two situations. The first is a cyber operation that is used to communicate a threat to use force (whether kinetic or cyber). The second is a threat conveyed by any means (e.g., public pronouncements) to carry out cyber operations qualifying as a use of force.

3. It is generally accepted that threats by States and officials in a position to make good those threats are lawful if the threatened action is itself lawful.117 There are two recognized exceptions to the international law prohibition on the use of force: the exercise of the right of self-defence and actions implementing a United Nations Security Council resolution under Chapter VII of the United Nations Charter (Rules 13 and 18). For instance, it would be lawful to threaten that a State will defend itself forcefully if attacked. Threatening other actions that do not violate international law would likewise be lawful.

4. Although threats are usually intended to be coercive in effect, there is no requirement that a specific 'demand' accompany the threat. The essence of a threat is that it is explicitly or impliedly communicative in nature. Actions which simply threaten the security of the target State, but which are not communicative in nature, do not qualify. For example, consider the case in which tensions between State A and State B are high. State A begins aggressively to develop the capability to conduct massive malicious cyber operations against State B. The mere acquisition of such capabilities that can be used to conduct uses of force does not constitute a threat. However, if the leader of State A announces, either on a conditional basis or otherwise, that the capabilities will be used for that purpose against State B, State A will be in violation of this Rule.

5. The International Group of Experts was divided as to whether a State manifestly lacking any capability to make good its threat, can violate this Rule. Despite the difference of opinion, it must be noted that cyber capability is not as dependent on a State's size, population, or economic and military capacity of a State as is the capacity to use conventional force. This means that it may be more difficult for a State to evaluate the capacity of another State to make good on its threat to use force by cyber means. Therefore, this issue plays a diminished role in evaluating cyber threats.

6. Similarly, no consensus could be achieved regarding a State that possesses the capability to carry out the threat but which clearly has no intention of doing so. An example would be that of a State that possesses an offensive cyber capability whose leader utters threats against other States for purely domestic political reasons.

7. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Rule 68 – Prohibition of threat or use of force

A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.

Rule 69 – Definition of use of force

A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.

Rule 70 – Definition of threat of force

A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force.

Rule 71 – Self-defence against armed attack
A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.

Rule 72 – Necessity and proportionality
A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate.

Rule 73 – Imminence and immediacy
The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy.

Rule 74 – Collective self-defence
The right of self-defence may be exercised collectively. Collective self-defence against a cyber operation amounting to an armed attack may only be exercised at the request of the victim State and within the scope of the request.

Rule 75 – Reporting measures of self-defence
Measures involving cyber operations undertaken by States in the exercise of the right of self-defence pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council.

Commentary to rule 82, para 14
To be 'armed', a conflict need not involve the employment of the armed forces. Nor is the involvement of the armed forces determinative. For example, should entities such as civilian intelligence agencies engage in cyber operations otherwise meeting the armed criterion …, an armed conflict may be triggered.

8. The Cyber Law Toolkit

'In the cyber context, States often act through non-State intermediaries and proxies. In such situations at the outset of an armed confrontation, the relevant State must exercise a sufficient degree of control over the non-State entity that commences hostilities against another State for the situation to qualify as an IAC. However, the correct legal test to use in this regard is the subject of an ongoing controversy. The prevailing standard for the characterization of an international armed conflict is that of "overall control", which requires that the State provides some support and that it participates in the organization, co-ordination, or planning of the relevant operations. A separate standard, the "effective control" test, requires that the State must exercise control over the entire course of the operations in question. While there is still disagreement as to whether the "effective control" test is the controlling test for the purposes of attribution under the law of State responsibility, there is consensus that the "overall control" test is the correct one for conflict qualification under IHL. The latter is also confirmed by decades of consistent practice by international criminal tribunals including the ICTY, the ECCC, and the ICC.'[173]

[173] The Cyber Law Toolkit, available at https://cyberlaw.ccdcoe.org/w/index.php?title=International_armed_conflict&mobileaction=toggle_view_desktop.

9. The Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States

'Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.'[174]

This provision is considered declaratory of customary international law, as also noted in the Case Concerning Armed Activities on the Territory of the Congo.[175]

10. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'[176]

11. International Court of Justice

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US), Judgement of 27 June 1986

115. The Court has taken the view (paragraph 110 above) that United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua. All the forms of United States participation mentioned above, and even the general control by the respondent State over a force with a high degree of dependency on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State. Such acts could well be committed by members of the contras without the control of the United States. For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.

176. As regards the suggestion that the areas covered by the two sources of law are identical, the Court observes that the United Nations Charter, the convention to which most of the United States argument is directed, by no means covers the whole area of the regulation of the use of force in international relations. On one essential point, this treaty itself refers to pre-existing customary international law; this reference to customary law is contained in the actual text of Article 51, which mentions the "inherent right" (in the French text the "droit naturel") of individual or collective self-defence, which "nothing in the present Charter shall impair" and which applies in

[174] United Nations General Assembly Resolution 2625 (XXV), 24 October 1970.
[175] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment of 19 December 2005, para. 162.
[176] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 24 June 2013, p. 8, para. 19.

the event of an armed attack. The Court therefore finds that Article 51 of the Charter is only meaningful on the basis that there is a "natural" or "inherent" right of self-defence, and it is hard to see how this can be other than of a customary nature, even if its present content has been confirmed and influenced by the Charter. Moreover the Charter, having itself recognized the existence of this right, does not go on to regulate directly all aspects of its content. For example, it does not contain any specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law. Moreover, a definition of the "armed attack" which, if found to exist, authorizes the exercise of the "inherent right" of self-defence, is not provided in the Charter, and is not part of treaty law. It cannot therefore be held that Article 51 is a provision which "subsumes and supervenes" customary international law. It rather demonstrates that in the field in question, the importance of which for the present dispute need hardly be stressed, customary international law continues to exist alongside treaty law. The areas governed by the two sources of law thus do not overlap exactly, and the rules do not have the same content. This could also be demonstrated for other subjects, in particular for the principle of non-intervention.

188. The Court thus finds that both Parties take the view that the principles as to the use of force incorporated in the United Nations Charter correspond, in essentials, to those found in customary international law. The Parties thus both take the view that the fundamental principle in this area is expressed in the terms employed in Article 2, paragraph 4, of the United Nations Charter. They therefore accept a treaty-law obligation to refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations. The Court has however to be satisfied that there exists in customary international law an opinio juris as to the binding character of such abstention. This opinio juris may, though with all due caution, be deduced from, inter alia, the attitude of the Parties and the attitude of States towards certain General Assembly resolutions, and particularly resolution 2625 (XXV) entitled "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations". The effect of consent to the text of such resolutions cannot be understood as merely that of a "reiteration or elucidation" of the treaty commitment undertaken in the Charter. On the contrary, it may be understood as an acceptance of the validity of the rule or set of rules declared by the resolution by themselves. The principle of non-use of force, for example, may thus be regarded as a principle of customary international law, not as such conditioned by provisions relating to collective security, or to the facilities or armed contingents to be provided under Article 43 of the Charter. It would therefore seem apparent that the attitude referred to expresses an opinio juris respecting such rule (or set of rules), to be thenceforth treated separately from the provisions, especially those of an institutional kind, to which it is subject on the treaty-law plane of the Charter.

189. As regards the United States in particular, the weight of an expression of opinion juris can similarly be attached to its support of the resolution of the Sixth International Conference of American States condemning aggression (18 February 1928) and ratification of the Montevideo Convention on Rights and Duties of States (26 December 1933). Article 11 of which imposes the obligation not to recognize territorial acquisitions or special advantages which have been obtained by force. Also significant is United States acceptance of the principle of the prohibition of the use of force which is contained in the declaration on principles governing the mutual relations of States participating in the Conference on Security and Co-operation in Europe (Helsinki, 1 August 1975), whereby the participating States undertake to "refrain in their mutual relations, as well as in their international relations in general, "(emphasis added) from the threat or use of force. Acceptance of a text in these terms confirms the existence of an opinio juris of the participating States prohibiting the use of force in international relations.

190. A further confirmation of the validity as customary international law of the principle of the prohibition of the use of force expressed in Article 2, paragraph 4, of the Charter of the United

Nations may be found in the fact that it is frequently referred to in statements by State representatives as being not only a principle of customary international law but also a fundamental or cardinal principle of such law. The International Law Commission, in the course of its work on the codification of the law of treaties, expressed the view that "the law of the Charter concerning the prohibition of the use of force in itself constitutes a conspicuous example of a rule in international law having the character of jus cogens" (paragraph (1) of the commentary of the Commission to Article 50 of its draft Articles on the Law of Treaties, ILC Yearbook, 1966-11, p. 247). Nicaragua in its Memorial on the Merits submitted in the present case States that the principle prohibiting the use of force embodied in Article 2, paragraph 4, of the Charter of the United Nations "has come to be recognized as jus cogens". The United States, in its Counter-Memorial on the questions of jurisdiction and admissibility, found it material to quote the views of scholars that this principle is a "universal norm", a "universal international law", a "universally recognized principle of international law", and a "principle of jus cogens".

191. As regards certain particular aspects of the principle in question, it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms. In determining the legal rule which applies to these latter forms, the Court can again draw on the formulations contained in the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (General Assembly resolution 2625 (XXV), referred to above). As already observed, the adoption by States of this text affords an indication of their opinio juris as to customary international law on the question. Alongside certain descriptions which may refer to aggression, this text includes others which refer only to less grave forms of the use of force. In particular, according to this resolution:

"Every State has the duty to refrain from the threat or use of force to violate the existing international boundaries of another State or as a means of solving international disputes, including territorial disputes and problems concerning frontiers of States.

States have a duty to refrain from acts of reprisal involving the use of force.

Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of that right to self-determination and freedom and independence.

Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State.

Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force."

193. The general rule prohibiting force allows for certain exceptions. In view of the arguments advanced by the United States to justify the acts of which it is accused by Nicaragua, the Court must express a view on the content of the right of self-defence, and more particularly the right of collective self-defence. First, with regard to the existence of this right, it notes that in the language of Article 51 of the United Nations Charter, the inherent right (or "droit naturel") which any State possesses in the event of an armed attack, covers both collective and individual self-defence. Thus, the Charter itself testifies to the existence of the right of collective self-defence in customary international law. Moreover, just as the wording of certain General Assembly declarations adopted by States demonstrates their recognition of the principle of the prohibition of force as definitely a matter of customary international law, some of the wording in those declarations

operates similarly in respect of the right of self-defence (both collective and individual). Thus, in the declaration quoted above on the Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, the reference to the prohibition of force is followed by a paragraph stating that: *"nothing in the foregoing paragraphs shall be construed as enlarging or diminishing in any way the scope of the provisions of the Charter concerning cases in which the use of force is lawful".* This resolution demonstrates that the States represented in the General Assembly regard the exception to the prohibition of force constituted by the right of individual or collective self-defence as already a matter of customary international law.

194. With regard to the characteristics governing the right of self-defence, since the Parties consider the existence of this right to be established as a matter of customary international law, they have concentrated on the conditions governing its use. In view of the circumstances in which the dispute has arisen, reliance is placed by the Parties only on the right of self-defence in the case of an armed attack which has already occurred, and the issue of the lawfulness of a response to the imminent threat of armed attack has not been raised. Accordingly the Court expresses no view on that issue. The Parties also agree in holding that whether the response to the attack is lawful depends on observance of the criteria of the necessity and the proportionality of the measures taken in self-defence. Since the existence of the right of collective self-defence is established in customary international law, the Court must define the specific conditions which may have to be met for its exercise, in addition to the conditions of necessity and proportionality to which the Parties have referred.

195. In the case of individual self-defence, the exercise of this right is subject to the State concerned having been the victim of an armed attack. Reliance on collective self-defence of course does not remove the need for this. There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein". This description, contained in Article 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces. But the Court does not believe that the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States. It is also clear that it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked. There is no rule in customary international law permitting another State to exercise the right of collective self-defence on the basis of its own assessment of the situation. Where collective self-defence is invoked, it is to be expected that the State for whose benefit this right is used will have declared itself to be the victim of an armed attack.

199. At all events, the Court finds that in customary international law, whether of a general kind or that particular to the inter-American legal system, there is no rule permitting the exercise of collective self-defence in the absence of a request by the State which regards itself as the victim of an armed attack. The Court concludes that the requirement of a request by the State which is the victim of the alleged attack is additional to the requirement that such a State should have declared itself to have been attacked.

228. Nicaragua has also claimed that the United States has violated Article 2, paragraph 4, of the Charter, and has used force against Nicaragua in breach of its obligation under customary international law in as much as it has engaged in "recruiting, training, arming, equipping, financing, supplying and otherwise encouraging, supporting, aiding, and directing military and paramilitary actions in and against Nicaragua" (Application, para. 26 (a) and (c)). So far as the claim concerns breach of the Charter, it is excluded from the Court's jurisdiction by the multilateral treaty reservation. As to the claim that United States activities in relation to the contras constitute a breach of the customary international law principle of the non-use of force, the Court finds that, subject to the question whether the action of the United States might be justified as an exercise of the right of self-defence, the United States has committed a prima facie violation of that principle by its assistance to the contras in Nicaragua, by "organizing or encouraging the organization of irregular forces or armed bands. . . for incursion into the territory of another State", and "participating in acts of civil strife . . . in another State", in the terms of General Assembly resolution 2625 (XXV). According to that resolution, participation of this kind is contrary to the principle of the prohibition of the use of force when the acts of civil strife referred to "involve a threat or use of force". In the view of the Court, while the arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all the assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua, as will be explained below, does not in itself amount to a use of force.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996

37. The Court will now address the question of the legality or illegality of recourse to nuclear weapons in the light of the provisions of the Charter relating to the threat or use of force.

38. The Charter contains several provisions relating to the threat and use of force. In Article 2, paragraph 4, the threat or use of force against the territorial integrity or political independence of another State or in any other manner inconsistent with the purposes of the United Nations is prohibited. That paragraph provides: *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."* This prohibition of the use of force is to be considered in the light of other relevant provisions of the Charter. In Article 51, the Charter recognizes the inherent right of individual or collective self-defence if an armed attack occurs. A further lawful use of force is envisaged in Article 42, whereby the Security Council may take military enforcement measures in conformity with Chapter VII of the Charter.

39. These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter.

41. The submission of the exercise of the right of self-defence to the conditions of necessity and proportionality is a rule of customary international law. As the Court stated in the case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America): there is a *"specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law"* (I. C. J. Reports 1986, p. 94, para. 176). This dual condition applies equally to Article 51 of the Charter, whatever the means of force employed.

Oil Platforms (Iran v. US), Merits, Judgment of 6 November 2003

51. Despite having thus referred to attacks on vessels and aircraft of other nationalities, the United States has not claimed to have been exercising collective self-defence on behalf of the neutral States engaged in shipping in the Persian Gulf; this would have required the existence of a request made to the United States *"by the State which regards itself as the victim of an armed attack"* (I. C. J. Reports 1986, p. 105, para. 199). Therefore, in order to establish that it was legally justified in attacking the Iranian platforms in exercise of the right of individual self-defence, the United States has to show that attacks had been made upon it for which Iran was responsible; and that those attacks were of such a nature as to be qualified as "armed attacks" within the meaning of that expression in Article 51 of the United Nations Charter, and as understood in customary law on the use of force. As the Court observed in the case concerning Military and Paramilitary Activities in and against Nicaragua, it is necessary to distinguish *"the most grave forms of the use of force (those constituting an armed attack) from other less grave forms"* (I. C. J. Reports 1986, p. 101, para. 191), since *"In the case of individual self-defence, the exercise of this right is subject to the State concerned having been the victim of an armed attack"* (ibid., p. 103, para. 195). The United States must also show that its actions were necessary and proportional to the armed attack made on it, and that the platforms were a legitimate military target open to attack in the exercise of self-defence.

72. The Court notes further that, as on the occasion of the earlier attack on oil platforms, the United States in its communication to the Security Council claimed to have been exercising the right of self-defence in response to the "attack" on the USS Samuel B. Roberts, linking it also with "a series of offensive attacks and provocations Iranian naval forces have taken against neutral shipping in the international waters of the Persian Gulf" (paragraph 67 above). Before the Court, it has contended, as in the case of the missile attack on the Sea Isle City, that the mining was itself an armed attack giving rise to the right of self-defence and that the alleged pattern of Iranian use of force "added to the gravity of the specific attacks, reinforced the necessity of action in self-defence, and helped to shape the appropriate response" (see paragraph 62 above). No attacks on United States-flagged vessels (as distinct from United States-owned vessels), additional to those cited as justification for the earlier attacks on the Reshadat platforms, have been brought to the Court's attention, other than the mining of the USS Samuel B. Roberts itself. The question is therefore whether that incident sufficed in itself to justify action in self-defence, as amounting to an "armed attack". The Court does not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the "inherent right of self-defence" ; but in view of all the circumstances, including the inconclusiveness of the evidence of Iran's responsibility for the mining of the USS Samuel B. Roberts, the Court is unable to hold that the attacks on the Salman and Nasr platforms have been shown to have been justifiably made in response to an "armed attack" on the United States by Iran, in the form of the mining of the USS Samuel B. Roberts.

73. As noted above (paragraph 43), in the present case a question of whether certain action is "necessary" arises both as an element of international law relating to self-defence and on the basis of the actual terms of Article XX, paragraph 1 (d), of the 1955 Treaty, already quoted, whereby the Treaty does "not preclude . . . measures . . . necessary to protect [the] essential security interests" of either party. In this latter respect, the United States claims that it considered in good faith that the attacks on the platforms were necessary to protect its essential security interests, and suggests that "A measure of discretion should be afforded to a party's good faith application of measures to protect its essential security interests." Iran was prepared to recognize some of the interests referred to by the United States - the safety of United States vessels and crew, and the uninterrupted flow of maritime commerce in the Persian Gulf - as being reasonable security interests of the United States, but denied that the United States actions against the platforms could be regarded as "necessary" to protect those interests. The Court does not however have to decide whether the United States interpretation of Article XX, paragraph 1 (d), on this point is correct, since the requirement of international law that measures taken avowedly in self-defence must have been necessary for that purpose is strict and objective, leaving no room for any "measure of

discretion". The Court will therefore turn to the criteria of necessity and proportionality in the context of international law on self-defence.

74. In its decision in the case concerning Military and Paramilitary Activities in and against Nicaragua, the Court endorsed the shared view of the parties to that case that in customary law "whether the response to the [armed] attack is lawful depends on observance of the criteria of the necessity and the proportionality of the measures taken in self-defence" (I. C.J. Reports 1986, p. 103, para. 194). One aspect of these criteria is the nature of the target of the force used avowedly in self-defence. In its communications to the Security Council, in particular in that of 19 October 1987 (paragraph 46 above), the United States indicated the grounds on which it regarded the Iranian platforms as legitimate targets for an armed action in self-defence. In the present proceedings, the United States has continued to maintain that they were such, and has presented evidence directed to showing that the platforms collected and reported intelligence concerning passing vessels, acted as a military communication link coordinating Iranian naval forces and served as actual staging bases to launch helicopter and small boat attacks on neutral commercial shipping. The United States has referred to documents and materials found by its forces aboard the vessel Iran Ajr (see paragraph 63 above), allegedly establishing that the Reshadat platforms served as military communication facilities. It has also affirmed that the international shipping community at the time was aware of the military use of the platforms, as confirmed by the costly steps commercial vessels took to avoid them, and by various witness reports describing Iranian attacks. The United States has also submitted expert analysis of the conditions and circumstances surrounding these attacks, examining their pattern and location in the light of the equipment at Iran's disposal. Finally, the United States has produced a number of documents, found on the Reshadat complex when it was attacked, allegedly corroborating the platforms' military function. In particular, it contends that these documents prove that the Reshadat platforms had monitored the movements of the Sea Isle City on 8 August 1987. On the other hand, the forces that attacked the Salman and Nasr complexes were not able to board the platforms containing the control centres, and did not therefore seize any material (if indeed such existed) tending to show the use of those complexes for military purposes.

76. The Court is not sufficiently convinced that the evidence available supports the contentions of the United States as to the significance of the military presence and activity on the Reshadat oil platforms; and it notes that no such evidence is offered in respect of the Salman and Nasr complexes. However, even accepting those contentions, for the purposes of discussion, the Court is unable to hold that the attacks made on the platforms could have been justified as acts of self-defence. The conditions for the exercise of the right of self-defence are well settled: as the Court observed in its Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons, "The submission of the exercise of the right of self-defence to the conditions of necessity and proportionality is a rule of customary international law" (Z. C. J. Reports 1996 (1), p. 245, para. 41); and in the case concerning Military and Paramilitary Activities in and against Nicaragua, the Court referred to a specific rule "whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it" as "a rule well established in customary international law" (I. C. J. Reports 1986, p. 94, para. 176). In the case both of the attack on the Sea Isle City and the mining of the USS Samuel B. Roberts, the Court is not satisfied that the attacks on the platforms were necessary to respond to these incidents. In this connection, the Court notes that there is no evidence that the United States complained to Iran of the military activities of the platforms, in the same way as it complained repeatedly of minelaying and attacks on neutral shipping, which does not suggest that the targeting of the platforms was seen as a necessary act. The Court would also observe that in the case of the attack of 19 October 1987, the United States forces attacked the R-4 platform as a "target of opportunity", not one previously identified as an appropriate military target (see paragraph 47 above).

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004

139. Under the terms of Article 51 of the Charter of the United Nations:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

Article 51 of the Charter thus recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it are imputable to a foreign State. The Court also notes that Israel exercises control in the Occupied Palestinian Territory and that, as Israel itself states, the threat which it regards as justifying the construction of the wall originates within, and not outside, that territory. The situation is thus different from that contemplated by Security Council resolutions 1368 (2001) and 1373 (200 l), and therefore lsrael could not in any event invoke those resolutions in support of its claim to be exercising a right of self-defence.

Armed Activities on the Territory of the Congo (DRC v. Uganda), Judgement of 19 December 2005

148. The prohibition against the use of force is a cornerstone of the United Nations Charter. Article 2, paragraph 4, of the Charter requires that:

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these parameters. Other means are available to a concerned State, including, in particular, recourse to the Security Council.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007

391. The first issue raised by this argument is whether it is possible in principle to attribute to a State conduct of persons — or groups of persons — who, while they do not have the legal status of State organs, in fact act under such strict control by the State that they must be treated as its organs for purposes of the necessary attribution leading to the State's responsibility for an internationally wrongful act. The Court has in fact already addressed this question, and given an answer to it in principle, in its Judgment of 27 June 1986 in the case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits, Judgment, I.C.J. Reports 1986, pp. 62-64). In paragraph 109 of that Judgment the Court stated that it had to

"determine . . . whether or not the relationship of the contras to the United States Government was so much one of dependence on the one side and control on the other that it would be right to equate the contras, for legal purposes, with an organ of the United States Government, or as acting on behalf of that Government" (p. 62).

Then, examining the facts in the light of the information in its possession, the Court observed that "there is no clear evidence of the United States having actually exercised such a degree of control

in all fields as to justify treating the contras as acting on its behalf" (para. 109), and went on to conclude that "the evidence available to the Court . . . is insufficient to demonstrate [the contras'] complete dependence on United States aid", so that the Court was "unable to determine that the contra force may be equated for legal purposes with the forces of the United States" (pp. 62- 63, para. 110).

399. This provision must be understood in the light of the Court's jurisprudence on the subject, particularly that of the 1986 Judgment in the case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) referred to above (paragraph 391). In that Judgment the Court, as noted above, after having rejected the argument that the contras were to be equated with organs of the United States because they were "completely dependent" on it, added that the responsibility of the Respondent could still arise if it were proved that it had itself "directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State" (I.C.J. Reports 1986, p. 64, para. 115); this led to the following significant conclusion: "For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed." (Ibid., p. 65.)

400. The test thus formulated differs in two respects from the test — described above — to determine whether a person or entity may be equated with a State organ even if not having that status under internal law. First, in this context it is not necessary to show that the persons who performed the acts alleged to have violated international law were in general in a relationship of "complete dependence" on the respondent State; it has to be proved that they acted in accordance with that State's instructions or under its "effective control". It must however be shown that this "effective control" was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.

United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment of 24 May 1980

58. No suggestion has been made that the militants, when they executed their attack on the Embassy, had any form of official status as recognised 'agents' or organs of the Iranian State. Their conduct in mounting the attack, overrunning the Embassy and seizing its inmates as hostages cannot, therefore, be regarded as imputable to that State on that basis. Their conduct might be considered as itself directly imputable to the Iranian State only if it were established that, in fact, on the occasion in question the militants acted on behalf of the State, having been charged by some competent organ of the Iranian State to carry out a specific operation. The information before the Court does not, however, suffice to establish with the requisite certainty the existence at that time of such a link between the militants and any competent organ of the State.

74. The policy thus announced by the Ayatollah Khomeini, of maintaining the occupation of the Embassy and the detention of its inmates as hostages for the purpose of exerting pressure on the United States Government was complied with by other Iranian authorities and endorsed by them repeatedly in statements made in various contexts. The result of that policy was fundamentally to transform the legal nature of the situation created by the occupation of the Embassy and the detention of its diplomatic and consular staff as hostages. The approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible.

12. International Criminal Tribunal for the former Yugoslavia

Prosecutor v. Duško Tadić, Case No. IT-94-1-A, Appeals Judgement, 15 July 1999

110. At one stage in the judgement, when dealing with the contras, the Court appeared tolay down a "dependence and control" test:

What the Court has to determine at this point is whether or not the relationship of the contras to the United States government was so much one of dependence on the one side and control on the other that it would be right to equate the contras, for legal purposes, with an organ of the United States government, or as acting on behalf of that Government**.**

111. The Prosecution, and Judge McDonald in her dissent, argue that by these words the Court set out an "agency test". According to them, the Court only resorted to the "effective control" standard once it had found no agency relationship between the contras and the United States to exist, so that the contras could not be considered organs of the United States. The Court, according to this argument, then considered whether specific operations of the contras could be attributed to the United States, and the standard it adopted for this attribution was the "effective control" standard.

112. The Appeals Chamber does not subscribe to this interpretation. Admittedly, in paragraph 115 of the Nicaragua judgement, where "effective control" is mentioned, it is unclear whether the Court is propounding "effective control" as an alternative test to that of "dependence and control" set out earlier in paragraph 109, or is instead spelling out the requirements of the same test. The Appeals Chamber believes that the latter is the correct interpretation. In Nicaragua, in addition to the "agency" test (properly construed, as shall be seen in the next paragraph, as being designed to ascertain whether or not an individual has the formal status of a State official), the Court propounded only the "effective control" test. This conclusion is supported by the evidently stringent application of the "effective control" test which the Court used in finding that the acts of the contras were not imputable to the United States.

114. On close scrutiny, and although the distinctions made by the Court might at first sight seem somewhat unclear, the contention is warranted that in the event, the Court essentially set out two tests of State responsibility: (i) responsibility arising out of unlawful acts of State officials; and (ii) responsibility generated by acts performed by private individuals acting as de facto State organs. For State responsibility to arise under (ii), the Court required that private individuals not only be paid or financed by a State, and their action be coordinated or supervised by this State, but also that the State should issue specific instructions concerning the commission of the unlawful acts in question. Applying this test, the Court concluded that in the circumstances of the case it was met as far as the UCLAs were concerned (who were paid and supervised by the United States and in addition acted under their specific instructions). By contrast, the test was not met as far as the contras were concerned: in their case no specific instructions had been issued by the United States concerning the violations of international humanitarian law which they had allegedly perpetrated.

The Grounds On Which the Nicaragua Test Does Not Seem To Be Persuasive

115. The "effective control" test enunciated by the International Court of Justice was regarded as correct and upheld by Trial Chamber II in the Judgement.137 The Appeals Chamber, with respect, does not hold the Nicaragua test to be persuasive. There are two grounds supporting this conclusion.

<u>a. The Nicaragua Test Would Not Seem to Be Consonant With the Logic of the Law of State Responsibility</u>

116. A first ground on which the Nicaragua test as such may be held to be unconvincing is based on the very logic of the entire system of international law on State responsibility.

117. The principles of international law concerning the attribution to States of acts performed by private individuals are not based on rigid and uniform criteria. These principles are reflected in Article 8 of the Draft on State Responsibility adopted on first reading by the United Nations International Law Commission and, even more clearly, in the text of the same provisions as provisionally adopted in 1998 by the ILC Drafting Committee.138 Under this Article, if it is proved that individuals who are not regarded as organs of a State by its legislation nevertheless do in fact act on behalf of that State, their acts are attributable to the State. The rationale behind this rule is to prevent States from escaping international responsibility by having private individuals carry out tasks that may not or should not be performed by State officials, or by claiming that individuals actually participating in governmental authority are not classified as State organs under national legislation and therefore do not engage State responsibility. In other words, States are not allowed on the one hand to act de facto through individuals and on the other to disassociate themselves from such conduct when these individuals breach international law. The requirement of international law for the attribution to States of acts performed by private individuals is that the State exercises control over the individuals. The degree of control may, however, vary according to the factual circumstances of each case. The Appeals Chamber fails to see why in each and every circumstance international law should require a high threshold for the test of control. Rather, various situations may be distinguished.

118. One situation is the case of a private individual who is engaged by a State to perform some specific illegal acts in the territory of another State (for instance, kidnapping a State official, murdering a dignitary or a high-ranking State official, blowing up a power station or, especially in times of war, carrying out acts of sabotage). In such a case, it would be necessary to show that the State issued specific instructions concerning the commission of the breach in order to prove – if only by necessary implication – that the individual acted as a de facto State agent. Alternatively it would be necessary to show that the State has publicly given retroactive approval to the action of that individual. A generic authority over the individual would not be sufficient to engage the international responsibility of the State. A similar situation may come about when an unorganised group of individuals commits acts contrary to international law. For these acts to be attributed to the State it would seem necessary to prove not only that the State exercised some measure of authority over those individuals but also that it issued specific instructions to them concerning the performance of the acts at issue, or that it ex post facto publicly endorsed those acts.

120. One should distinguish the situation of individuals acting on behalf of a State without specific instructions, from that of individuals making up an organised and hierarchically structured group, such as a military unit or, in case of war or civil strife, armed bands of irregulars or rebels. Plainly, an organised group differs from an individual in that the former normally has a structure, a chain of command and a set of rules as well as the outward symbols of authority. Normally a member of the group does not act on his own but conforms to the standards prevailing in the group and is subject to the authority of the head of the group. Consequently, for the attribution to a State of acts of these groups it issufficient to require that the group as a whole be under the overall control of the State.

121. This kind of State control over a military group and the fact that the State is held responsible for acts performed by a group independently of any State instructions, or even contrary to instructions, to some extent equates the group with State organs proper. Under the rules of State responsibility, as restated in Article 10 of the Draft on State Responsibility as provisionally adopted by the International Law Commission,139 a State is internationally accountable for ultra vires acts or transactions of its organs. In other words it incurs responsibility even for acts committed by its officials outside their remit or contrary to its behest. The rationale behind this provision is that a State must be held accountable for acts of its organs whether or not these organs complied with instructions, if any, from the higher authorities. Generally speaking, it can be maintained that the whole body of international law on State responsibility is based on a realistic concept of accountability, which disregards legal formalities and aims at ensuring that States

entrusting some functions to individuals or groups of individuals must answer for their actions, even when they act contrary to their directives.

122. The same logic should apply to the situation under discussion. As noted above, the situation of an organised group is different from that of a single private individual performing a specific act on behalf of a State. In the case of an organised group, the group normally engages in a series of activities. If it is under the overall control of a State, it must perforce engage the responsibility of that State for its activities, whether or not each of them was specifically imposed, requested or directed by the State. To a large extent the wise words used by the United States-Mexico General Claims Commission in the Youmans case with regard to State responsibility for acts of State military officials should hold true for acts of organised groups over which a State exercises overall control.

123. What has just been said should not, of course, blur the necessary distinction between the various legal situations described. In the case envisaged by Article 10 of the Draft on State Responsibility (as well as in the situation envisaged in Article 7 of the same Draft), State responsibility objectively follows from the fact that the individuals who engage in certain internationally wrongful acts possess, under the relevant legislation, the status of State officials or of officials of a State's public entity. In the case under discussion here, that of organised groups, State responsibility is instead the objective corollary of the overall control exercised by the State over the group. Despite these legal differences, the fact nevertheless remains that international law renders any State responsible for acts in breachof international law performed (i) by individuals having the formal status of organs of a State (and this occurs even when these organs act ultra vires or contra legem), or (ii) by individuals who make up organised groups subject to the State's control. International law does so regardless of whether or not the State has issued specific instructions to those individuals. Clearly, the rationale behind this legal regulation is that otherwise, States might easily shelter behind, or use as a pretext, their internal legal system or the lack of any specific instructions in order to disclaim international responsibility.

b. The Nicaragua Test is at Variance With Judicial and State Practice

124. There is a second ground – of a similarly general nature as the one just expounded - on which the Nicaragua test as such may be held to be unpersuasive. This ground is determinative of the issue. The "effective control" test propounded by the International Court of Justice as an exclusive and all-embracing test is at variance with international judicial and State practice: such practice has envisaged State responsibility in circumstances where a lower degree of control than that demanded by the Nicaragua test was exercised. In short, as shall be seen, this practice has upheld the Nicaragua test with regard to individuals or unorganised groups of individuals acting on behalf of States. By contrast, it has applied a different test with regard to military or paramilitary groups.

125. In cases dealing with members of military or paramilitary groups, courts have clearly departed from the notion of "effective control" set out by the International Court of Justice (i.e., control that extends to the issuance of specific instructions concerning the various activities of the individuals in question). Thus, for instance, in the Stephens case, the Mexico-United States General Claims Commission attributed to Mexico acts committed during a civil war by a member of the Mexican "irregular auxiliary" of the army, which among other things lacked both uniforms and insignia.142 In this case the Commission did not enquire as to whether or not specific instructions had been issued concerning the killing of the United States national by that guard.

126. Similarly, in the Kenneth P. Yeager case, 143 the Iran-United States Claims Tribunal ("Claims Tribunal") held that wrongful acts of the Iranian "revolutionary guards" or "revolutionary Komitehs" vis-à-vis American nationals carried out between 13 and 17 February 1979 were attributable to Iran…Iran, the respondent State, had argued that the conduct of those "Guards" was not attributable to it. It had admitted that "revolutionary guards and Komiteh personnel were engaged in the maintenance of law and order from January 1979 to months after February 1979 as government police forces rapidly lost control over the situation." It had asserted, however, that

"these revolutionaries did not operate under the name 'Revolutionary Komitehs' or 'Revolutionary Guards', and that they were not affiliated with the Provisional Government".144 In other words, the "Guards" were "not authentic";145 hence, their conduct was not attributable to Iran. The Claims Tribunal considered instead that the acts were attributable to Iran because the "Guards" or "Komitehs" had acted as de facto State organs of Iran.

130. Precisely what measure of State control does international law require for organised military groups? Judging from international case law and State practice, it would seem that for such control to come about, it is not sufficient for the group to be financially or even militarily assisted by a State. This proposition is confirmed by the international practice concerning national liberation movements. Although some States provided movements such as the PLO, SWAPO or the ANC with a territorial base or with economic and military assistance (short of sending their own troops to aid them), other States, including those against which these movements were fighting, did not attribute international responsibility for the acts of the movements to the assisting States.157 Nicaragua also supports this proposition, since the United States, although it aided the contras financially, and otherwise, was not held responsible for their acts (whereas on account of this financial and other assistance to the contras, the United States was held by the Court to be responsible for breaching the principle of non-intervention as well as "its obligation ?...g not to use force against another State."158 This was clearly a case of responsibility for the acts of its own organs).

131. In order to attribute the acts of a military or paramilitary group to a State, it must be proved that the State wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity. Only then can the State be held internationally accountable for any misconduct of the group. However, it is not necessary that, in addition, the State should also issue, either to the head or to members of the group, instructions for the commission of specific acts contrary to international law.

132. It should be added that courts have taken a different approach with regard to individuals or groups not organised into military structures. With regard to such individuals or groups, courts have not considered an overall or general level of control to be sufficient, but have instead insisted upon specific instructions or directives aimed at the commission of specific acts, or have required public approval of those acts following their commission.

133. The Appeals Chamber will mention, first of all, the United States Diplomatic and Consular Staff in Tehran case.159 There, the International Court of Justice rightly found that the Iranian students (who did not comprise an organised armed group) who had stormed the United States embassy and taken hostage 52 United States nationals, had not initially acted on behalf of Iran, for the Iranian authorities had not specifically instructed them to perform those acts.160 Nevertheless, Iran was held internationally responsible for failing to prevent the attack on the United States' diplomatic premises and subsequently to put an end to that attack.161 Later on, the Iranian authorities formally approved and endorsed the occupation of the Embassy and the detention of the United States nationals by the militants and even went so far as to order the students not to put an end to that occupation. At this stage, according to the Court, the militants became de facto agents of the Iranian State and their acts became internationally attributable to that State.

137. In sum, the Appeals Chamber holds the view that international rules do not always require the same degree of control over armed groups or private individuals for the purpose of determining whether an individual not having the status of a State official under internal legislation can be regarded as a de facto organ of the State. The extent of the requisite State control varies. Where the question at issue is whether a single private individual or a group that is not militarily organised has acted as a de facto State organ when performing a specific act, it is necessary to ascertain whether specific instructions concerning the commission of that particular act had been issued by that State to the individual or group in question; alternatively, it must be established whether the unlawful act had been publicly endorsed or approved ex post facto by the

State at issue. By contrast, control by a State over subordinate armed forces or militias or paramilitary units may be of an overall character (and must comprise more than the mere provision of financial assistance or military equipment or training).

138. Of course, if, as in Nicaragua, the controlling State is not the territorial State where the armed clashes occur or where at any rate the armed units perform their acts, more extensive and compelling evidence is required to show that the State is genuinely in control of the units or groups not merely by financing and equipping them, but also by generally directing or helping plan their actions.

141. It should be added that international law does not provide only for a test of overall control applying to armed groups and that of specific instructions (or subsequent public approval), applying to single individuals or militarily unorganised groups. The Appeals Chamber holds the view that international law also embraces a third test. This test is the assimilation of individuals to State organs on account of their actual behaviour within the structure of a State (and regardless of any possible requirement of State instructions).

145. In the light of the above discussion, the following conclusion may be safely reached. In the case at issue, given that the Bosnian Serb armed forces constituted a "military organization", the control of the FRY authorities over these armed forces required by international law for considering the armed conflict to be international was overall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations. By contrast, international rules do not require that such control should extend to the issuance of specific orders or instructions relating to single military actions, whether or not such actions were contrary to international humanitarian law.

Prosecutor v Milutinović et al, Case No. IT-05-87-T, Trial Judgment, 26 February 2009

125. The existence of an armed conflict does not depend upon the views of the parties to the conflict.

13. United Nations

During the 2003 Iraq conflict, Kofi Annan, Secretary-General of the United Nations, stated: 'No principle of the Charter is more important than the principle of the non-use of force as embodied in Article 2, paragraph 4 […]. Secretaries-General confront many challenges in the course of their tenures but the challenge that tests them and defines them inevitably involves the use of force.'[177]

14. NATO

Warsaw Summit Communiqué[178]

The heads of state and government 'reaffirm NATO's defensive mandate', that 'cyber defence is part of NATO's core task of collective defence', and that NATO is ready for the Allies to invoke collective defence in response to a significant cyberattack, the equivalent of an armed attack through cyberspace. The Allies now 'recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea'.[179]

---

[177] Ralph Zacklin, The United Nations Secretariat and the Use of Force in a Unipolar World: Power v. Principle, CUP, 2010, pp. xii-xiii.

[178] Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, paragraphs 70-71, available at https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[179] Ibid.

Brussels Summit Declaration[180]

20. Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive, and coercive. NATO will continue to adapt to the evolving cyber threat landscape, which is affected by both state and non-state actors, including state-sponsored. Cyber defence is part of NATO's core task of collective defence […]. *We reaffirm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable*. We also support work to maintain international peace and security in cyberspace and to promote stability and reduce the risk of conflict, recognising that we all stand to benefit from a norms-based, predictable, and secure cyberspace. We will further develop our partnership with industry and academia from all Allies to keep pace with technological advances through innovation.

21. Our nations have come under increasing challenge from both state and non-state actors who use hybrid activities that aim to create ambiguity and blur the lines between peace, crisis, and conflict. While the primary responsibility for responding to hybrid threats rests with the targeted nation, NATO is ready, upon Council decision, to assist an Ally at any stage of a hybrid campaign. *In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of armed attack*. We are enhancing our resilience, improving our situational awareness, and strengthening our deterrence and defence posture. We are also expanding the tools at our disposal to address hostile hybrid activities. We announce the establishment of Counter Hybrid Support Teams, which provide tailored, targeted assistance to Allies, upon their request, in preparing for and responding to hybrid activities. We will continue to support our partners as they strengthen their resilience in the face of hybrid challenges.

15. European Union

Joint Communication to the European Parliament, the European Council and the Council

'Hybrid activities by State and non-state actors continue to pose a serious and acute threat to the EU and its Member States. Our societies face a serious challenge from those who seek to damage the EU and its Member States, from cyber-attacks disrupting the economy and public services, through targeted disinformation campaigns to hostile military actions. Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by both state and non-state actors. The nerve agent attack in Salisbury last March1 further underlined the versatility of hybrid threats and the multitude of tactics now available. In response, the European Council highlighted the need to step up the capacity of the EU and its Member States to detect, prevent and respond to hybrid threats in areas such as cyber, strategic communication and counter-intelligence. It also drew particular attention to the need for resilience in the face of Chemical, Biological, Radiological and Nuclear-related threats.'[181]

[180] Brussels Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, available at https://www.nato.int/cps/en/natohq/official_texts_156624.htm (emphasis added).

[181] Increasing resilience and bolstering capabilities to address hybrid threats, Brussels, 13.6.2018 JOIN(2018) 16 final, Joint Communication to the European Parliament, the European Council and the Council, p. 1, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0016&from=cs.

16. Literature

Books

GRAY, Christine D. *International law and the use of force.* Fourth edition. Oxford: Oxford University Press, 2018, pp. 489. ISBN 978-0-19-880841-1.

RUYS, Tom; CORTEN, Olivier. *The use of force in international law: a case-based approach.* First edition. Oxford: Oxford University Press, 2018, pp. 948. ISBN 978-0-19-878436-4.

WELLER, Marc; SOLOMOU, Alexia; RYLATT, Jake William. *The Oxford handbook of the use of force in international law.* First edition. New York: Oxford University Press, 2015, pp. 1280. Oxford handbooks. ISBN 978-0-19-880621-9.

ROSCINI, Marco. *Cyber operations and the use of force in international law.* First edition. Oxford: Oxford University Press, 2014, pp. 307. ISBN 978-0-19-965501-4.

GEERS, Kenneth (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*. New York: Cambridge University Press, 2012.

Simma, Bruno., Mosler, Hermann., Paulus, Andreas. and Chaitidou, Elini. (n.d.). *The Charter of the United Nations: A Commentary*. 2012, 3nd Edition. Oxford University Press.

Zemanek, Karl. Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law*, 2010.

Articles

Corn, Gary; Jensen, Eric. The Use of Force and Cyber Countermeasures Notes & Comments. Temple International & Comparative Law Journal, 2018, Vol. 32, pp. 127-134.

Nguyen, Reese. *Navigating "Jus Ad Bellum" in the Age of Cyber Warfare.* California Law Review, 2013, Vol. 101, Issue 4, pp. 1079-1129.

Buchan, Russell. *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?* Journal of Conflict and Security Law, 2012, Vol. 17, Issue 2, pp. 212-227.

Delibasis, Dimitrios. *The Right of States to Use Force in Cyberspace: Defining the Rules of Engagement.* Information & Communications Technology Law, 2002, Vol. 11, Issue 3, pp. 255-268.

Schmitt, Michael N. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.* Columbia Journal of Transnational Law, 1999, Vol. 37, Issue 3, pp. 885-938.

Dinstein, Yoram*. Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*. International Law Studies, 2013, Vol. 89, p. 280.

Condron, Sean. *Getting it right: Protecting American Critical Infrastructure In Cyberspace*. Harvard Journal of Law & Technology, 2007, Vol. 20.

DEVER, John; DEVER, James. *Cyberwarfare: Attribution, Preemption, and National Self Defense*. Cyber Warfare, Vol. 2, p. 40.

Dev, Priyanka R. *"Use of Force" and "armed attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing need for Formal U.N. Response*. Texas International law Journal, 215, vol. 50.

CHIRCOP, Luke. *A Due Diligence Standard of Attribution in Cyberspace*. International and Comparative Law Quarterly, 2018, Vol. 67, Issue 3,pp. 643–668.

Cordula Droege. *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*.) International Review of the Red Cross, 2012, Vol. 94.

MAČÁK, Kubo. *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*. Journal of Conflict and Security Law, 2016, Vol. 21, Issue 3, pp. 405–428.

MAČÁK, Kubo. *From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers*. Leiden Journal of International Law, 2017, Vol. 30, Issue 4, pp. 877–899.

MAGLARAS, Leandros et al. Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. ICST Transactions on Security and Safety, 2018, Vol. 5, Issue 16.

MUDRINICH, Erik M. *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*. The Air Force Law Review, 2012, Vol. 68, p. 167.

SOMER, Jonathan. *Acts of Non-State Armed Groups and the Law Governing Armed Conflict*. American Society of International Law, 2006.

RUYS, Tom. *The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are Minimal Uses of Force Excluded from UN Charter Article 2(4)?* The American Journal of International Law. 2014, Vol. 108.

SCHMITT, Michael. *Classification of Cyber Conflict*. Journal of Conflict and Security Law. 2012, Vol. 17, Issue 2, pp. 245-260.

SHARP, Walter. *Cyberspace and the Use of Force*. VA: Aegis Research Corp., 1999.

BUCHAN, Russel. *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?* Journal of Conflict and Security Law, 2012, Vol. 17, Issue 2, pp. 211–227.

COLLINS, Sean a McCOMBIE, Stephen. *Stuxnet: the emergence of a new cyber weapon and its implications*. Journal of Policing, Intelligence and Counter Terrorism. 2012, Vol. 7, Issue 1.

DELUCA, Christopher D. The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. Pace International Law Review Online Companion. 2013, Vol. 3, Issue 9, p. 315.

FOLTZ, Andrew. *Stuxnet, "Schmitt Analysis", and the Cyber "Use of Force" Debate*. Air War College. 2012.

HATHAWAY, Oona et al. *Law of Cyber-Attack*. Faculty Scholarship Series. 2012. https://digitalcommons.law.yale.edu/fss_papers/3852

HOISINGTON, Mathew. *Cyberwarfare and the Use of Force Giving Rise to the Right of Selfdefense*. Boston Colledge International and Comparative Law Review. 2009, Vol. 32, Issue 2, pp. 439-454.

JENSEN, Eric Talbot. *Computer Attacks on National Infrastructure: A Use of Force Invoking the Right of Self-Defense*. Stanford Journal of International Law. 2002, Vol. 28, pp. 207 – 240.

KOH, Harold Hongju. *International Law in Cyberspace*. Harvard International Law Journal. 2012, Vol. 54.

KUTA, Martin, PÍŠA, Radek, NOVÁK, Adam. Kyberterorismus – Uvod do problematiky, podoby a přehled aktů kybernetického terorismu, kybernetická bezpečnost, mezinárodní srovnání. *Parlamentní institut: srovnávací studie č. 5.383*. 2019.

LIN, Herbert. *Offensive Cyber Operations and the Use of Force*. Journal of National Security Law & Policy. 2010, p. 77.

MCGAVRAN, Wolfgang. *Intended Consequences: Regulating Cyber Attacks*. Tulane Journal of Technology and Intellectual Property. 2009, p. 265.

NOVÁK, Tomáš. *Informační operace na pozadí současných ozbrojených konfliktů*. Vojenské rozhledy. 2014, Vol. 23 (55), Issue 4, pp. 51-62.

OTTIS, Rain. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

UHLÍŘOVÁ, Kateřina. Zásada zákazu použití síly a „počítačový útok" proti kritickým infrastrukturám státu: vacuum iuris či výkladová výzva? In: KYSELOVSKÁ, T., SEHNÁLEK, D., ROZEHNALOVÁ, N. (eds.). *In Varietate Concordia: soubor vědeckých statí k poctě prof. Vladimíra Týče*. Brno: Masarykova univerzita, 2019, pp. 413-464.

SILVER, Daniel. Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter. In: SCHMITT, Michael a T. O'DONELL, Brian. *Computer Network Attack and International Law*. Naval War College International Law Studies, 2002.

SCHMITT, Michael. *The Law of Cyber Warfare: Quo Vadis?* Stanford Law and Policy Review. 2014, Vol. 25, Issue 2, p. 280.

WEISSBRODT, David. *Cyber-Conflict, Cyber-Crime, and CyberEspionage*. Minnesota Journal of International Law. 2013, Vol. 22, pp. 349-350.

Critical Infrastructures

Don Ferguson

1. Introduction

1.1. Focus

The focus of this chapter is on EU cybersecurity legislation and guidance directed specifically at critical infrastructures, and the essential services they provide. In terms of EU sector-specific cybersecurity legislation, the focus is on the electricity sector, as network and information systems may be dependent on the electricity sector.

1.2. Approach

The EU legislation and guidance will be presented in the following order:

- enforcement,
- general requirements, and
- sector-specific requirements: the electricity sector.

2. Enforcement

DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

(…)

Whereas:

(1) The objectives of this Directive are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).

(2) Information systems are a key element of political, social and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of those systems in the Union is vital for the development of the internal market and of a competitive and innovative economy. Ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime.

(3) Attacks against information systems, and, in particular, attacks linked to organised crime, are a growing menace in the Union and globally, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the

critical infrastructure of Member States and of the Union. This constitutes a threat to the achievement of a safer information society and of an area of freedom, security, and justice, and therefore requires a response at Union level and improved cooperation and coordination at international level.

(4) There are a number of critical infrastructures in the Union, the disruption or destruction of which would have a significant cross-border impact. It has become apparent from the need to increase the critical infra structure protection capability in the Union that the measures against cyber attacks should be complemented by stringent criminal penalties reflecting the gravity of such attacks. Critical infrastructure could be understood to be an asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

(5) There is evidence of a tendency towards increasingly dangerous and recurrent large-scale attacks conducted against information systems which can often be critical to Member States or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called 'botnets', which involves several stages of a criminal act, where each stage alone could pose a serious risk to public interests. This Directive aims, inter alia, to introduce criminal penalties for the creation of botnets, namely, the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber attacks. Once created, the infected network of computers that constitute the botnet can be activated without the computer users' knowledge in order to launch a large-scale cyber attack, which usually has the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, such as disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information.

(6) Large-scale cyber attacks can cause substantial economic damage both through the interruption of information systems and communication and through the loss or alteration of commercially important confidential information or other data. Particular attention should be paid to raising the awareness of innovative small and medium-sized enterprises to threats relating to such attacks and their vulnerability to such attacks, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security.

(…)

(13) It is appropriate to provide for more severe penalties where an attack against an information system is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime (1), where a cyber attack is conducted on a large scale, thus affecting a significant number of information systems, including where it is intended to create a botnet, or where a cyber attack causes serious damage, including where it is carried out through a botnet. It is also appropriate to provide for more severe penalties where an attack is conducted against a critical infrastructure of the Member States or of the Union.

(…)

(26) In order to fight cybercrime effectively, it is necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against cyber attacks. Member States should take the necessary measures to protect their critical infrastructure from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection and security of information systems by legal persons, for example in connection with the provision of publicly

available electronic communications services in accordance with existing Union legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations. The cost and burden of such protection should be proportionate to the likely damage a cyber attack would cause to those affected. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks.

(…)

Article 1. Subject matter
This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

Article 2. Definitions
For the purposes of this Directive, the following definitions shall apply:

(a) 'information system' means a device or group of inter- connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;

(b) 'computer data' means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function;

(c) 'legal person' means an entity having the status of legal person under the applicable law, but does not include States or public bodies acting in the exercise of State authority, or public international organisations;

(d) 'without right' means conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.

Article 3. Illegal access to information systems
Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.

Article 4. Illegal system interference
Member States shall take the necessary measures to ensure that seriously hindering or interrupting the functioning of an information system by inputting computer data, by trans mitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 5. Illegal data interference
Member States shall take the necessary measures to ensure that deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data

inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 6. Illegal interception
Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 7. Tools used for committing offences
Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:

(a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Article 8. Incitement, aiding and abetting and attempt
1. Member States shall ensure that the incitement, or aiding and abetting, to commit an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

2. Member States shall ensure that the attempt to commit an offence referred to in Articles 4 and 5 is punishable as a criminal offence.

Article 9. Penalties
1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, proportionate and dissuasive criminal penalties.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum term of imprisonment of at least two years, at least for cases which are not minor.

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years where:

(a) they are committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;

(b) they cause serious damage; or

(c) they are committed against a critical infrastructure information system.

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this

may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.

(…)

COUNCIL REGULATION (EU 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

(…)

Whereas:

(1) On 18 October 2018 the European Council adopted conclusions which called for the work on the capacity to respond to and deter cyber-attacks through Union restrictive measures to be taken forward, further to the Council conclusions of 19 June 2017.

(2) On 17 May 2019 the Council adopted Decision (CFSP) 2019/797. Decision (CFSP) 2019/797 establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. Persons, entities and bodies subject to the restrictive measures are listed in the Annex to that Decision.

(3) This Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and to a fair trial and the right to the protection of personal data. This Regulation should be applied in accordance with those rights.

(4) The power to establish and amend the list in Annex I to this Regulation should be exercised by the Council in order to ensure consistency with the process for establishing, amending and reviewing the Annex to Decision (CFSP) 2019/797.

(5) For the implementation of this Regulation, and in order to ensure maximum legal certainty within the Union, the names and other relevant data concerning natural and legal persons, entities and bodies whose funds and economic resources are to be frozen in accordance with this Regulation should be made public. Any processing of personal data should comply with Regulations (EU) 2016/679 (2) and (EU) 2018/1725 (3) of the European Parliament and of the Council.

(6) Member States and the Commission should inform each other of the measures taken pursuant to this Regulation and of other relevant information at their disposal in connection with this Regulation.

(7) Member States should lay down rules on sanctions applicable to infringements of the provisions of this Regulation and make sure that they are implemented. Those sanctions should be effective, proportionate and dissuasive,

(…)

Article 1

1. This Regulation applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.

2. Cyber-attacks constituting an external threat include those which:

(a) originate, or are carried out, from outside the Union;

(b) use infrastructure outside the Union;

(c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or

(d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union.

3. For this purpose, cyber-attacks are actions involving any of the following:

(a) access to information systems;

(b) information system interference;

(c) data interference; or

(d) data interception,

where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.

4. Cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia:

(a) critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people;

(b) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned;

(c) critical State functions, in particular in the areas of defence, governance and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions;

(d) the storage or processing of classified information; or

(e) government emergency response teams.

5. Cyber-attacks constituting a threat to the Union include those carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its common security and defence policy (CSDP) operations and missions and its special representatives.

6. Where deemed necessary to achieve common foreign and security policy (CFSP) objectives in the relevant provisions of Article 21 of the Treaty on European Union, restrictive measures under this Regulation may also be applied in response to cyber-attacks with a significant effect against third States or international organisations.

7. For the purposes of this Regulation, the following definitions apply:

(a) 'information systems' means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes digital data, as well as digital data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;

(b) 'information system interference' means hindering or interrupting the functioning of an information system by inputting digital data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;

(c) 'data interference' means deleting, damaging, deteriorating, altering or suppressing digital data on an information system, or rendering such data inaccessible; it also includes theft of data, funds, economic resources or intellectual property;

(d) 'data interception' means intercepting, by technical means, non-public transmissions of digital data to, from or within an information system, including electromagnetic emissions from an information system carrying such digital data.

8. For the purposes of this Regulation, the following additional definitions apply:

(a) 'claim' means any claim, whether asserted by legal proceedings or not, made before or after the date of entry into force of this Regulation, under or in connection with a contract or transaction, and includes in particular:

(i) a claim for performance of any obligation arising under or in connection with a contract or transaction;

(ii) a claim for extension or payment of a bond, financial guarantee or indemnity of whatever form;

(iii) a claim for compensation in respect of a contract or transaction;

(iv) a counterclaim;

(v) a claim for the recognition or enforcement, including by the procedure of exequatur, of a judgment, an arbitration award or an equivalent decision, wherever made or given;

(b) 'contract or transaction' means any transaction of whatever form and whatever the applicable law, whether comprising one or more contracts or similar obligations made between the same or different parties; for this purpose, 'contract' includes a bond, guarantee or indemnity, particularly a financial guarantee or financial indemnity, and credit, whether legally independent or not, as well as any related provision arising under, or in connection with, the transaction;

(c) 'competent authorities' refers to the competent authorities of the Member States as identified on the websites listed in Annex II;

(d) 'economic resources' means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but may be used to obtain funds, goods or services;

(e) 'freezing of economic resources' means preventing the use of economic resources to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them;

(f) 'freezing of funds' means preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character or destination or any other change that would enable the funds to be used, including portfolio management;

(g) 'funds' means financial assets and benefit of every kind, including, but not limited to:

(i) cash, cheques, claims on money, drafts, money orders and other payment instruments;

(ii) deposits with financial institutions or other entities, balances on accounts, debts and debt obligations;

(iii) publicly-and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts;

(iv) interest, dividends or other income on or value accruing from or generated by assets;

(v) credit, right of set-off, guarantees, performance bonds or other financial commitments;

(vi) letters of credit, bills of lading and bills of sale; and

(vii) documents showing evidence of an interest in funds or financial resources;

(h) 'territory of the Union' means the territories of the Member States to which the Treaty is applicable, under the conditions laid down in the Treaty, including their airspace.

Article 2
The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include any of the following:

(a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;

(b) the number of natural or legal persons, entities or bodies affected;

(c) the number of Member States concerned;

(d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;

(e) the economic benefit gained by the perpetrator, for himself or for others;

(f) the amount or nature of data stolen or the scale of data breaches; or

(g) the nature of commercially sensitive data accessed.

Article 3
1. All funds and economic resources belonging to, owned, held or controlled by any natural or legal person, entity or body listed in Annex I shall be frozen.

2. No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of natural or legal persons, entities or bodies listed in Annex I.

3. Annex I shall include, as identified by the Council in accordance with Article 5(1) of Decision (CFSP) 2019/797:

(a) natural or legal persons, entities or bodies who are responsible for cyber-attacks or attempted cyber-attacks;

(b) natural persons or legal persons, entities or bodies that provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;

(c) natural or legal persons, entities or bodies associated with the natural or legal persons, entities or bodies covered by points (a) and (b) of this paragraph.

(…)

Article 18
This Regulation shall apply:

(a) within the territory of the Union, including its airspace;

(b) on board any aircraft or vessel under the jurisdiction of a Member State;

(c) to any natural person inside or outside the territory of the Union who is a national of a Member State;

(d) to any legal person, entity or body, inside or outside the territory of the Union, which is incorporated or constituted under the law of a Member State;

(e) to any legal person, entity or body in respect of any business done in whole or in part within the Union.

(…)

COUNCIL IMPLEMENTING REGULATION (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

(…)

Whereas:

(1) On 17 May 2019 the Council adopted Regulation (EU) 2019/796.

(2) Targeted restrictive measures against cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States are among the measures included in the Union's framework for a joint diplomatic response to malicious cyber-activities (the cyber diplomacy toolbox) and are a vital instrument to deter and respond to such activities. Restrictive measures can also be applied in response to cyber-attacks with a significant effect against third States or international organisations, where deemed necessary to achieve common foreign and security policy objectives set out in the relevant provisions of Article 21 of the Treaty on European Union.

(3) On 16 April 2018 the Council adopted conclusions in which it firmly condemned the malicious use of information and communications technologies, including in the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', which caused significant damage and economic loss in the Union and beyond. On 4 October 2018 the Presidents of the European Council and of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') expressed serious concerns in a joint statement about an attempted cyber-attack to undermine the integrity of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands, an aggressive act which demonstrated contempt for the solemn purpose of the OPCW. In a declaration made on behalf of the Union on 12 April 2019, the High Representative urged actors to stop undertaking malicious cyber-activities that aim to undermine the Union's integrity, security and economic competiveness, including acts of cyber-enabled theft of intellectual property. Such cyber-enabled thefts include those carried out by the actor publicly known as 'APT10' ('Advanced Persistent Threat 10').

(4) In this context, and to prevent, discourage, deter and respond to continuing and increasing malicious behaviour in cyberspace, six natural persons and three entities or bodies should be included in the list of natural and legal persons, entities and bodies subject to restrictive measures set out in Annex I to Regulation (EU) 2019/796. Those persons and entities or bodies are responsible for, provided support for or were involved in, or facilitated cyber-attacks or attempted cyber-attacks, including the attempted cyber-attack against the OPCW and the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', as well as 'Operation Cloud Hopper'.

(5) Regulation (EU) 2019/796 should therefore be amended accordingly,

(…)

Article 1

Annex I to Regulation (EU) 2019/796 is amended in accordance with the Annex to this Regulation. (…)

ANNEX

(…)

B. Legal persons, entities and bodies

	Name	Identifying information	Reasons	Date of listing
(…)				
2.	Chosun Expo	a.k.a.: Chosen Expo; Korea Export Joint Venture Location: DPRK	Chosun Expo provided financial, technical or material support for and facilitated a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as "WannaCry" and cyber-attacks against the Polish Financial Supervision Authority and Sony Pictures Entertainment, as well as cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank. "WannaCry" disrupted information systems around the world by targeting information systems with ransomware and blocking access to data. It affected information systems of companies in the Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States. The actor publicly known as "APT38" ("Advanced Persistent Threat 38") or the "Lazarus Group" carried out "WannaCry". Chosun Expo can be linked to APT38 / the Lazarus Group, including through the accounts used for the cyber-attacks.	30.7.2020
3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Address: 22 Kirova Street, Moscow, Russian Federation	The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known by its field post number 74455, is responsible for cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and for cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as "NotPetya" or "EternalPetya" in June 2017 and the cyber-attacks directed at an Ukrainian power grid in the winter of 2015 and 2016. "NotPetya" or "EternalPetya" rendered data inaccessible in a number of companies in the Union, wider Europe and worldwide, by targeting	30.7.2020

			computers with ransomware and blocking access to data, resulting amongst others in significant economic loss. The cyber-attack on a Ukrainian power grid resulted in parts of it being switched off during winter. The actor publicly known as "Sandworm" (a.k.a. "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" and "Telebots"), which is also behind the attack on the Ukrainian power grid, carried out "NotPetya" or "EternalPetya". The Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation has an active role in the cyber-activities undertaken by Sandworm and can be linked to Sandworm.	

3. General requirements

COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

(…)

Whereas:

(1) In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infra structures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

(2) On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasised.

(3) In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European programme for critical infrastructure protection ('EPCIP') and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority.

(4) In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection.

(5) This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector.

(6) The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures.

(7) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such ECIs should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures should be done under a common minimum approach. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute a well-established and efficient means of dealing with transboundary critical infrastructures. EPCIP should build on such cooperation. Information pertaining to the designation of a particular infrastructure as an ECI should be classified at an appropriate level in accordance with existing Community and Member State legislation.

(8) Since various sectors have particular experience, expertise and requirements concerning critical infrastructure protection, a Community approach to critical infrastructure protection should be developed and implemented taking into account sector specificities and existing sector based measures including those already existing at Community, national or regional level, and where relevant cross-border mutual aid agreements between owners/operators of critical infrastructures already in place. Given the very significant private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery, a Community approach needs to encourage full private sector involvement.

(9) In terms of the energy sector and in particular the methods of electricity generation and transmission (in respect of supply of electricity), it is understood that where deemed appropriate, electricity generation may include electricity transmission parts of nuclear power plants, but exclude the specifically nuclear elements covered by relevant nuclear legislation including treaties and Community law.

(10) This Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms are already in place, they should continue to be used and will contribute to the overall implementation of this Directive. Duplication of, or contradiction between, different acts or provisions should be avoided.

(11) Operator security plans ('OSPs') or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritisation of counter measures and procedures should be in place in all designated ECIs. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated ECIs possess relevant OSPs or similar measures. Where such plans do not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the establishment of OSPs.

(12) Measures, principles, guidelines, including Community measures as well as bilateral and/or multilateral cooperation schemes that provide for a plan similar or equivalent to an OSP or provide for a Security Liaison Officer or equivalent, should be deemed to satisfy the requirements of this Directive in relation to the OSP or the Security Liaison Officer respectively.

(13) Security Liaison Officers should be identified for all designated ECIs in order to facilitate cooperation and communication with relevant national critical infra structure protection authorities. With a view to avoiding unnecessary work and duplication, each Member State should

first assess whether the owners/operators of designated ECIs already possess a Security Liaison Officer or equivalent. Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers.

(14) The efficient identification of risks, threats and vulnerabilities in the particular sectors requires communication both between owners/operators of ECIs and the Member States, and between the Member States and the Commission. Each Member State should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified, including where relevant information on possible improvements in the ECIs and cross-sector dependencies, which could be the basis for the development of specific proposals by the Commission on improving the protection of ECIs, where necessary.

(15) In order to facilitate improvements in the protection of ECIs, common methodologies may be developed for the identification and classification of risks, threats and vulnerabilities to infrastructure assets.

(16) Owners/operators of ECIs should be given access primarily through relevant Member State authorities to best practices and methodologies concerning critical infrastructure protection.

(17) Effective protection of ECIs requires communication, coordination, and cooperation at national and Community level. This is best achieved through the nomination of European critical infrastructure protection contact points ('ECIP contact points') in each Member State, who should coordinate European critical infrastructure protection issues internally, as well as with other Member States and the Commission.

(18) In order to develop European critical infrastructure protection activities in areas which require a degree of confidentiality, it is appropriate to ensure a coherent and secure information exchange in the framework of this Directive. It is important that the rules of confidentiality according to applicable national law or Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents are observed with regard to specific facts about critical infrastructure assets, which could be used to plan and act with a view to causing unacceptable consequences for critical infrastructure installations. Classified information should be protected in accordance with relevant Community and Member State legislation. Each Member State and the Commission should respect the relevant security classification given by the originator of a document.

(19) Information sharing regarding ECIs should take place in an environment of trust and security. The sharing of information requires a relationship of trust such that companies and organisations know that their sensitive and confidential data will be sufficiently protected.

(20) Since the objectives of this Directive, namely the creation of a procedure for the identification and designation of ECIs, and a common approach to the assessment of the need to improve the protection of such infrastructures, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale of the action, be better achieved at Community level, the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(21) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union,

(…)

Article 1. Subject matter
This Directive establishes a procedure for the identification and designation of European critical infrastructures ('ECIs'), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people.

Article 2. Definitions
For the purpose of this Directive:

(a) 'critical infrastructure 'means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;

(b) 'European critical infrastructure 'or 'ECI 'means critical infra structure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

(c) 'risk analysis 'means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;

(d) 'sensitive critical infrastructure protection related information 'means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;

(e) 'protection 'means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;

(f) 'owners/operators of ECIs 'means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.

Article 3. Identification of ECIs
1. Pursuant to the procedure provided in Annex III, each Member State shall identify potential ECIs which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Article 2(a) and (b).

The Commission may assist Member States at their request to identify potential ECIs.

The Commission may draw the attention of the relevant Member States to the existence of potential critical infrastructures which may be deemed to satisfy the requirements for designation as an ECI.

Each Member State and the Commission shall continue on an ongoing basis the process of identifying potential ECIs.

2. The cross-cutting criteria referred to in paragraph 1 shall comprise the following:

(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

(c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Member States concerned by a

particular critical infrastructure. Each Member State shall inform the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

The sectoral criteria shall take into account the characteristics of individual ECI sectors.

The Commission together with the Member States shall develop guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds to be used to identify ECIs. The criteria shall be classified. The use of such guidelines shall be optional for the Member States.

3. The sectors to be used for the purposes of implementing this Directive shall be the energy and transport sectors. The subsectors are identified in Annex I.

If deemed appropriate and in conjunction with the review of this Directive as laid down in Article 11, subsequent sectors to be used for the purpose of implementing this Directive may be identified. Priority shall be given to the ICT sector.

Article 4. Designation of ECIs

1. Each Member State shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI.

2. Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI. The Commission may participate in these discussions but shall not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure.

A Member State that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State on whose territory the potential ECI is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this issue. The Commission shall without delay communicate this wish to the Member State on whose territory the potential ECI is located and endeavour to facilitate agreement between the parties.

3. The Member State on whose territory a potential ECI is located shall designate it as an ECI following an agreement between that Member State and those Member States that may be significantly affected.

The acceptance of the Member State on whose territory the infrastructure to be designated as an ECI is located, shall be required.

4. The Member State on whose territory a designated ECI is located shall inform the Commission on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated ECI. Only those Member States that may be significantly affected by an ECI shall know its identity.

5. The Member States on whose territory an ECI is located shall inform the owner/operator of the infrastructure concerning its designation as an ECI. Information concerning the designation of an infrastructure as an ECI shall be classified at an appropriate level.

6. The process of identifying and designating ECIs pursuant to Article 3 and this Article shall be completed by 12 January 2011 and reviewed on a regular basis.

Article 5. Operator security plans

1. The operator security plan (‘OSP’) procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II.

2. Each Member State shall assess whether each designated ECI located on its territory possesses an OSP or has in place equivalent measures addressing the issues identified in Annex II. If a Member State finds that such an OSP or equivalent exists and is updated regularly, no further implementation action shall be necessary.

3. If a Member State finds that such an OSP or equivalent has not been prepared, it shall ensure by any measures deemed appropriate, that the OSP or equivalent is prepared addressing the issues identified in Annex II.

Each Member State shall ensure that the OSP or equivalent is in place and is reviewed regularly within one year following designation of the critical infrastructure as an ECI. This period may be extended in exceptional circumstances, by agreement with the Member State authority and with a notification to the Commission.

4. In a case where supervisory or oversight arrangements already exist in relation to an ECI such arrangements are not affected by this Article and the relevant Member State authority referred to in this Article shall be the supervisor under those existing arrangements.

5. Compliance with measures including Community measures which in a particular sector require, or refer to a need to have, a plan similar or equivalent to an OSP and oversight by the relevant authority of such a plan, is deemed to satisfy all the requirements of Member States under, or adopted pursuant to, this Article. The guidelines for application referred to in Article 3(2) shall contain an indicative list of such measures.

Article 6. Security Liaison Officers

1. The Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority.

2. Each Member State shall assess whether each designated ECI located on its territory possesses a Security Liaison Officer or equivalent. If a Member State finds that such a Security Liaison Officer is in place or an equivalent exists, no further implementation action shall be necessary.

3. If a Member State finds that a Security Liaison Officer or equivalent does not exist in relation to a designated ECI, it shall ensure by any measures deemed appropriate, that such a Security Liaison Officer or equivalent is designated.

4. Each Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned. This communication mechanism shall be without prejudice to national requirements concerning access to sensitive and classified information.

5. Compliance with measures including Community measures which in a particular sector require, or refer to a need to have, a Security Liaison Officer or equivalent, is deemed to satisfy all the requirements of Member States in, or adopted pursuant to, this Article. The guidelines for application referred to in Article 3(2) shall contain an indicative list of such measures.

Article 7. Reporting

1. Each Member State shall conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors.

2. Each Member State shall report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated pursuant to Article 4 and is located on its territory.

A common template for these reports may be developed by the Commission in cooperation with the Member States.

Each report shall be classified at an appropriate level as deemed necessary by the originating Member State.

3. Based on the reports referred to in paragraph 2, the Commission and the Member States shall assess on a sectoral basis whether further protection measures at Community level should be considered for ECIs. This process shall be undertaken in conjunction with the review of this Directive as laid down in Article 11.

4. Common methodological guidelines for carrying out risk analyses in respect of ECIs may be developed by the Commission in cooperation with the Member States. The use of such guidelines shall be optional for the Member States.

Article 8. Commission support for ECIs
The Commission shall support, through the relevant Member State authority, the owners/operators of designated ECIs by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection.

Article 9. Sensitive European critical infrastructure protection-related information
1. Any person handling classified information pursuant to this Directive on behalf of a Member State or the Commission shall have an appropriate level of security vetting.

Member States, the Commission and relevant supervisory bodies shall ensure that sensitive European critical infrastructure protection-related information submitted to the Member States or to the Commission is not used for any purpose other than the protection of critical infrastructures.

2. This Article shall also apply to non-written information exchanged during meetings at which sensitive subjects are discussed.

Article 10. European critical infrastructure protection contact points
1. Each Member State shall appoint a European critical infrastructure protection contact point ('ECIP contact point').

2. ECIP contact points shall coordinate European critical infrastructure protection issues within the Member State, with other Member States and with the Commission. The appointment of an ECIP contact point does not preclude other authorities in a Member State from being involved in European critical infrastructure protection issues.

(…)

ANNEX I

List of ECI sectors

Sector I Energy

Subsector 1. Electricity: Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity

Subsector 2. Oil: Oil production, refining, treatment, storage and transmission by pipelines

Subsector 3. Gas: Gas production, refining, treatment, storage and transmission by pipelines; LNG terminals

Sector II Transport

Subsector 4. Road transport

Subsector 5. Rail transport

Subsector 6. Air transport

Subsector 7. Inland waterways transport

Subsector 8. Ocean and short-sea shipping and ports

The identification by the Member States of critical infrastructures which may be designated as ECIs is undertaken pursuant to Article 3. Therefore the list of ECI sectors in itself does not generate a generic obligation to designate an ECI in each sector.

ANNEX II

ECI OSP PROCEDURE

The OSP will identify critical infrastructure assets and which security solutions exist or are being implemented for their protection. The ECI OSP procedure will cover at least:

1. identification of important assets;

2. conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and

3. identification, selection and prioritisation of counter-measures and procedures with a distinction between:

- permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,

- graduated security measures, which can be activated according to varying risk and threat levels.

ANNEX III

Procedure for the identification by the Member States of critical infrastructures which may be designated as an ECI pursuant to Article 3

Article 3 requires each Member State to identify the critical infrastructures which may be designated as an ECI. This procedure shall be implemented by each Member State through the following series of consecutive steps.

A potential ECI which does not satisfy the requirements of one of the following sequential steps is considered to be 'non-ECI 'and is excluded from the procedure. A potential ECI which does satisfy the requirements shall be subjected to the next steps of this procedure.

Step 1

Each Member State shall apply the sectoral criteria in order to make a first selection of critical infrastructures within a sector.

Step 2

Each Member State shall apply the definition of critical infrastructure pursuant to Article 2(a) to the potential ECI identified under step 1.

The significance of the impact will be determined either by using national methods for identifying critical infrastructures or with reference to the cross-cutting criteria, at an appropriate national level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 3

Each Member State shall apply the transboundary element of the definition of ECI pursuant to Article 2(b) to the potential ECI that has passed the first two steps of this procedure. A potential ECI which does satisfy the definition will follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 4

Each Member State shall apply the cross-cutting criteria to the remaining potential ECIs. The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI.

A potential ECI which has passed through this procedure shall only be communicated to the Member States which may be significantly affected by the potential ECI.

Commission Staff Working Document: Evaluation of Council Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection

{SWD(2019) 310 final}

(...)

Glossary

CI: Critical infrastructure

CIP: Critical infrastructure protection

CIP PoC: Critical Infrastructure Protection Point-of-Contact

CIPS: EU Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks

CIWIN: Critical Infrastructure Warning Information Network

ECI: European critical infrastructure

ECIP: European Critical Infrastructure Protection

EEAS: European External Action Service

EPCIP: European Programme for Critical Infrastructure Protection

ERNCIP: European Reference Network for Critical Infrastructure Protection

ICT: Information and communications technology

ISF: Internal Security Fund

MFF: Multiannual Financial Framework

NCI: National critical infrastructure

NIS: Network sand information system

OSP: Operator Security Plan

PPP: Public-private partnership

SLO: Security Liaison Officer

1. Introduction

1.1 Context, Purpose and Scope of the Evaluation

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (hereafter referred to as the European Critical Infrastructure (ECI) Directive or simply the Directive) aims to enhance the protection of critical infrastructure in the European Union, the disruption or destruction of which would have significant cross-border impacts. The Directive achieves this through the creation of a procedure for the identification and designation of ECIs, and a common approach to the assessment of the need to improve the protection of such infrastructure. The Directive: sets out a number of key definitions; provides procedures for the identification and designation of critical infrastructure that may be designated as European critical infrastructure (ECI); puts in place certain requirements for ECI owners/operators and Member States; creates national points-of-contact; and extends various kinds of Commission support to Member States. The Directive is part of the European Programme for Critical Infrastructure Protection (EPCIP, hereafter referred to as the Programme), which was established in 2006 and which sets out an overall policy approach and framework for critical infrastructure protection (CIP) activities in the EU.

The Directive was subject to review in 2012 in accordance with Article 11. The review found that although the Directive was quickly transposed in the national laws of all Member States, its application was limited, with only a few potential ECI having been identified and even fewer ultimately designated. There were also considerable discrepancies in the application of the Directive by different Member States and few indications that it had actually improved security in the transport and energy sectors. Furthermore, the evaluation found that the Directive's sector-focused approach posed a challenge to some Member States that approached the task of analysing criticalities on a cross-sectoral rather than sector-specific basis. Finally, the review found that the Directive primarily fostered bilateral rather than pan- European cooperation on CIP-related matters, but also that insufficient consideration had been given to the links between critical infrastructures (CIs) in different sectors or across national boundaries. The results of the review prompted the Commission to pilot a new approach to the implementation of the Programme in 2013 in order to emphasise the interdependencies that exist both between different sectors and between CIs, industry, and state actors, and that threats to one type of CI can have a significant impact on a broad range of actors involved in the operation of other CIs but more widely as well.

In the meantime, the threat picture facing CI was changing. For instance, the 2017 Comprehensive Assessment of EU Security Policy underlined the new and evolving challenges faced by the European Union, including from terrorism, emerging technologies (e.g. unmanned aerial vehicles), insiders, etc. The Comprehensive Assessment pointed to the need to take a broad view on the protection of CI in the EU, starting with the evaluation of the Directive. Preparations for the evaluation began in early 2018.

In late August 2018, the European Commission launched the evaluation of the Directive, which aimed to analyse its implementation and application in each EU Member State according to a number of specific criteria set out in the Commission's Better Regulation Guidelines, namely relevance, coherence, effectiveness, efficiency, EU added value and sustainability. The evaluation would also: analyse the scope and content of the Directive; the organisation of work at the national and EU level aimed at implementing the Directive; and the state of implementation of the Directive's provisions. The evaluation was in part informed by an external study of the Directive's implementation.

The overall purpose of the evaluation was to provide the Commission with a qualitative and quantitative analysis of the Directive as well as recommendations as to how to further strengthen the protection and resilience of CI. While the evaluation was not focused on other non-legislative elements of the Programme, certain elements of the Programme were accounted for as appropriate.

The evaluation considered the implementation of the Directive from its entry into force in January 2009 to the start of the evaluation in August 2018. A wide range of stakeholders were consulted as part of the evaluation. These included: competent authorities at the Member State level; CI operators and other industry stakeholders in the transport and energy sectors; academia and think tanks; the general public; and the relevant Directorate-Generals within the Commission, the European External Action Service (EEAS), and EU Agencies.

The evaluation accounted for the aforementioned 2012 review of the Directive. It also took into account other relevant EU instruments that entered into force since 2008 and that deal either directly or indirectly with the protection and resilience of CI. The evaluation assessed the extent to which these instruments can be considered to be redundant, complementary, or obstacles to the effective implementation of the Directive, and whether there were any evident gaps.

This staff working document describes the evaluation, how it was carried out, and what it found. It is accompanied by four annexes that contain procedural information, a summary of the consultations, an overview of the methodology, and a detailed description of the evaluation criteria.

2. Background to the Intervention

2.1 Context

In June 2004, the European Council called for the preparation of an overall strategy to protect critical infrastructure in Europe. On 20 October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism. This put forward suggestions on how to enhance European efforts to prevent, prepare for and respond to terrorist attacks involving CI. In December 2004, the Council endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection. In November 2019 [*sic.*], the Commission published a Green Paper on a European Programme for Critical Infrastructure Protection.

In December 2006, the Commission issued a Communication on a European Programme for Critical Infrastructure Protection.11 This set out an overall policy approach and framework for CIP activities in the EU. The Programme's four main pillars would be:

- A procedure for the identification and designation of European critical infrastructure (ECI) and for the assessment of the need to improve their protection (provided for in the ECI Directive adopted in 2008);

- Measures designed to facilitate the implementation of the Programme, including an Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of a CIP expert group

at EU level, a CIP information-sharing process, and the identification and analysis of interdependencies;

- Funding for CIP-related measures and projects focusing on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks 'for the period 2007-2013; and

- The development of an external dimension in recognition of the interconnected and interdependent nature of societies both within and beyond the EU. The external dimension would entail cooperation with third countries outside the EU through measures such as sector-specific memoranda of understanding and encouraging the raising of CIP standards outside of the EU.

Following the creation of the Programme in 2006, CIWIN and the CIP expert group were established. The CIPS funding also came available and the Programme's external dimension was activated. At the same time, the Commission was developing the proposal for a mechanism that would provide a procedure for ECI identification and designation. In December 2006, the Commission published a Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

2.2 Key Elements of the Intervention

The Directive that was adopted in 2008 establishes a procedure for identifying and designating European critical infrastructure and a common approach for assessing the need to improve their protection. The Directive has a sectoral scope, applying only to the energy and transport sectors. However, provisions were made for the possible expansion of the Directive to apply to other sectors.

Under the Directive, each Member State on whose territory a potential ECI is located should inform and engage in bilateral and/or multilateral discussions with those Member States most likely to be significantly affected by the disruption/destruction of potential ECI. While the Directive allows for the Commission to participate in these discussions, it does not grant the Commission access to detailed information that could allow for the unequivocal identification of infrastructures that Member States have identified as potential ECIs.

Under the Directive, the Member State on whose territory a potential ECI is located designates it as an ECI following an agreement between that Member State and other Member States that risk being significantly affected. The Directive also requires owners/operators of designated ECI to prepare Operator Security Plans (OSP) (i.e. advanced business continuity plans) and to designate Security Liaison Officers (SLO), the task of which is to serve as a link between the owner/operator and the competent authority responsible for CIP at national level.

The OSP should contain a procedure enabling ECI owners/operators to identify CI assets and which security solutions exist and/or are being implemented for their protection. Within one year of designating CI as ECI, the Member State shall check that an OSP or equivalent is in place and that it is reviewed regularly. The Directive stipulates that appropriate action must be taken by the Member State where ECI owners/operators do not fulfil the OSP requirement.

The SLO function is intended to serve as a point-of-contact between the ECI owner/operator and the competent authority on issues relating to security. According to the Directive, each Member State should assess whether any designated ECI on its territory has an SLO or equivalent, and take steps where this is not the case. Each Member State shall ensure that an appropriate communication mechanism exists between the SLO and the competent national authority by which relevant security-related information (e.g. threats/risks to designated ECI) can be exchanged).

Finally, each Member State must designate a European Critical Infrastructure Protection (ECIP) contact point responsible for coordinating CIP issues with European relevance at Member State level, with other Member States, and vis-à-vis the Commission.

2.3 Evolution of the Context

The evaluation at hand was launched in light of a significantly changed context compared with when the Directive was adopted in 2008. First of all, a number of CIP-relevant sectoral initiatives in the energy and transport sectors have been taken at EU level in recent years. Besides these, the Network and Information Security (NIS) Directive was adopted in 2016. This aims to achieve a high level of security of network and information systems on the part of essential service providers in a total of seven sectors including transport and energy.

Furthermore, the threat picture facing CI in Europe has evolved, as has European thinking on how best to manage threats. Although the nature of the antagonistic, accidental man-made and natural threats to CI have changed little since the mid-2000s, the risk for certain types of incidents (e.g. hybrid threats, insiders, cyberattacks) has increased. All the while, digital infrastructure has grown in importance, both as a basis for the operation of CI and as CI in its own right. While recent technological innovations like 5G, unmanned aircraft systems, and artificial intelligence are likely to bring further efficiencies to CI operations, they may also pose serious threats in the hands of malicious actors interested in disrupting CI operations. Finally, CIs, both in Europe and further afield, are increasingly interconnected and reliant upon one another. The more complex these interdependencies, the more infrastructure in disparate (and at first glance seemingly peripheral) sectors might be considered critical. As such, there is increasing interest on the part of Member States and CI owners/operators in ensuring that infrastructures are resilient, meaning that they are equipped to 'bounce back 'from disruption as quickly as possible.

2.4 Intervention Logic and Baseline

2.4.1 Intervention Logic

(...)

The intervention logic helps in visualising the problem that the Directive was intended to address when it was first adopted, namely an inadequate level of protection of CIs with a European dimension in the energy and transport sectors in the face of natural disasters, technological threats, and man-made threats, including terrorism.

Three primary drivers prompted the Commission to put forward its proposal for a Directive. The first related to the existence of different levels of protection of CIs in different parts of the Union. This was of concern given the fact that the damage or loss of CI in one Member State could have adverse effects on CI in other Member States, but also potentially at a more regional or even pan-European level (with the potential to impact the entire European economy) as well. In parallel with the development of ever-deeper interdependencies between CIs in different Member States, the early 2000s was a period of increasing market liberalization (e.g. in electricity and gas supply) and the introduction of many new technologies that facilitated CI operations and made them more efficient. Taken together, these developments had the combined effect of drawing CI in different parts of the EU together into larger, more interconnected networks.

At the same time, the responsibilities of CI owners/operators varied or were unclear across the Union. This was in part due to the decentralisation of control over CI as a result of market liberalization and the privatization of CI. The absence of a clear, harmonised regulatory framework across the Union risked creating uncertainty on the part of CI operators, especially in instances where they sought to operate CI in different Member States with different standards/requirements.

The fragmentation of CI operations across Europe also meant that CI owners/operators were subject to different obligations/requirements depending on where within the Union they worked.

This had the effect of creating an uneven playing field within the internal market. Variation as to how different Member States regulated/oversaw different CI sectors had certain economic implications for CI owners/operators.

In recognition of the problem and the various imperatives to act (the drivers), the Commission saw the need for action with the objective of improving the level of protection for European critical infrastructures by creating a horizontal framework for the identification and designation of ECIs and for the assessment of the needs to improve their protection. The Commission's proposal for the Directive emphasised the need to account for particular experience, expertise and requirements concerning CIP in different sectors, and that any new EU approach to CIP should be developed and implemented taking into account sectoral specificities and existing measures. Annex I of the Commission's proposal identified 11 'critical infrastructure sectors, 'of which the transport and energy sectors were deemed to be immediate priorities for action. In the ECI Directive as it was adopted, the focus was on these two sectors, though provisions were made for the possible expansion of the Directive to apply to other sectors, of which the ICT sector was to be given priority. The specific objectives of the Directive were twofold: to establish a procedure for the identification and designation of ECIs; and to establish a common approach to the assessment of the need to improve the protection of ECIs.

The Directive's general and specific objectives were to be achieved through a number of provisions included in the legislation that provided the Member States with common definitions related to CIP that would enable them to more easily carry out discussions over Member State lines in order to jointly identify CIs with potentially serious cross-border implications if disrupted in one way or another. Through these discussions, the Commission aimed to enable the Member States to formally designate such CIs as 'European 'in nature and ensure that enhanced protective measures were subsequently taken. The Commission also saw the need to support ECI owners/operators as necessary, to stimulate EU-wide exchange on CIP-relevant issues, and to maintain a general overview of the threats, risks and vulnerabilities facing specific sectors in which CIs with European implications operated. The provisions in the Directive addressing these imperatives are referred to as inputs in the intervention logic and include: the provision of scope (limited to the transport and energy sectors) and definitions (e.g. 'critical infrastructure, ' 'European critical infrastructure'); a procedure for the identification of CI which may be designated as ECI; a corresponding procedure for the designation of critical infrastructure as ECI; specific requirements for designated ECI owners/operators (e.g. to develop and maintain an OSP, to create an SLO function); and reporting requirements for both competent authorities and ECI owners/operators. It also creates an ECIP contact point group, and obligates the Commission to provide support to ECIs upon request (for instance by providing access to available best practices and methodologies, supporting training and the exchange of information on relevant technical developments related to CIP, etc.). Through these provisions (inputs), the Directive should yield an equal number of corresponding outputs (see Figure 1, above).

The intervention logic makes clear that where these outputs are met, the Directive should generate a number of results/outcomes that address both the general problem and drivers that prompted the Commission to take the initiative in the first place. The expected results/outcomes include: progress towards the achievement of common levels of protection of ECIs throughout the EU; the definition of clear and similar responsibilities and common procedures applying to all ECI stakeholders; and enhanced protection of the stability of the internal market. Assuming these results/outcomes are achieved, the Directive should ultimately lead to an improved level of protection of ECIs in the energy and transport sectors, but also stronger protection of the stability of the European internal market, thereby resolving the initial identified problem.

2.4.2 Baseline

The amount of information concerning national-level CIP measures prior to the Directive coming into force (and that was needed in order to establish a baseline for comparison) was found to be limited. The evaluation addressed this by using information provided by the Member States 'CIP

points-of-contact (CIP PoCs) to partially reconstruct the pre-Directive situation at national level. This information was then combined with other sources of information, allowing for an investigation as to whether the key elements introduced by the Directive were present at Member State level prior to 2008. By analysing the information provided by the CIP PoCs via the online survey and the feedback gathered as part of the case studies included in the external study with information contained in the implementation tables, it was possible to describe the general nature of national CIP measures before 2008, (…)

The findings show that in half of the Member States (14), there was no definition as to what exactly constitutes a critical infrastructure before 2008. There were no specific laws/measures in place intended to identify/protect CI in 14 Member States. Meanwhile, 10 Member States did not have any formalised cooperative arrangements with other Member States in order to exchange CIP-relevant information.

On the other hand, the analysis revealed that most Member States performed threat assessments in the energy and transport sectors, and that many had developed national-level cooperation mechanisms regarding CIP. Meanwhile, most Member States (25) had in place OSP-equivalent requirements before the introduction of the Directive, and a majority of Member States (20) already required functions similar to the SLO provision at key CI facilities.

It is important to point out that the baseline situation described above is by no means intended to describe the maturity or effectiveness of the different Member States 'CIP frameworks before 2008. For instance, the absence of elements mandated by the Directive from certain national frameworks prior to 2008 is by no means to suggest that these national approaches were any less effective than those in Member States where such elements were present.

3. Implementation State of Play

3.1 Implementation and Transposing Measures

The Directive was adopted in December 2008, and entered into force the following month (January 2009). Member States were given until 12 January 2011 to transpose the Directive into national law. The Member States 'approaches to transposition took three general forms, namely: 1) transposition of the Directive as part of broader national CIP frameworks; 2) the introduction of ECI-specific measures (i.e. national legislation focusing exclusively/almost entirely on ECI); and, 3) the introduction of sector-specific (energy and/or transport) legislation.

The majority of Member States (18) opted to transpose the Directive within the fold of national CIP legislation. This was done either through amendments to existing national legislation (in most cases aimed at providing clarification in view of the contents of the Directive) or through new legislation. The remaining Member States transposed the Directive either through ECI-specific measures or sector-specific legislation (four and six Member States, respectively). No matter which path the Member States chose, most of the work associated with transposition was carried out during the first few years after the Directive was adopted, the main exception being Croatia, which passed a comprehensive law on CI in 2013 (the same year that it joined the EU) and subsequently began transposing the Directive.

3.2 Definitions and Scope

National transposition efforts have primarily focused on the definitions of CI and ECI, respectively. While several Member States (12) opted to introduce the same (or quite similar) definitions as those proposed in the Directive, others (four, all of which made amendments to administrative provisions) opted not to include definitions when transposing the Directive.

Generally speaking, there is a certain degree of variation as to how different Member States understand the notion of CI. This is clearly reflected in how the term has been defined at national

level. For 10 Member States, CI consists of both assets and systems, which puts their definitions in line with the definition provided in the Directive. In other Member States, the CI definition focuses solely on their systemic character, while in others still, an asset-focused definition is applied. Differences in how the Member States define CI is more than a matter of semantics; the decision to define CI as assets indicates a focus on the protection of specific components, while ones emphasising the systems that they comprise point to a broader approach where CIs are the means by which the continuity of certain vital services is assured.

The different definitions used by the Member States also revealed different perspectives as to what reliable CI functionality is expected to ensure on a societal basis. For instance, the definitions used by most Member States associated CI with things like 'vital societal functions', 'health', 'safety', 'security', and 'economic or social well-being '(all of which are mentioned in the Directive). Six Member States linked CI with economic stability as well, while another three Member States associate the protection of CI with continuity of government and/or the continued existence of the nation.

Less variance was observed in terms of the definition of ECI. Most Member States adopted the same definition of ECI as in the Directive. Some Member States opted not to introduce the definition, or introduced an abridged definition of ECI. Other definitions included in the Directive (e.g. 'protection 'of CI, 'sensitive information', 'risk analysis', 'owners/operators of ECI') were in some cases directly transposed. A total of 11 Member States introduced additional definitions, including 'cross-cutting and sectoral criteria', 'competent authorities/stakeholders', 'critical zones', 'emergency', 'essential service', 'cybersecurity', and 'negative effect/spill-over'.

In implementing the Directive, most Member States included provisions pertaining to the energy and transport sectors and the related sub-sectors listed in the Directive, with some of these providing additional sectoral specificity.

With regard to the energy sector, a significant majority of the Member States (24) specified the sub-sectors that fell within the scope of national-level measures. In most cases, the three energy sub-sectors named in the Directive (electricity, oil and gas) were all deemed to be in scope. In the case of three Member States, the transposition legislation made clear that the energy sector was in scope, though no specific sub-sectors were indicated. More variation was observed within the transport sector, with the air transport sub-sector most often cited in national transposition legislation (19), followed by inland waterways (14), sea transport (16), and rail transport (17). For obvious reasons, the type of transport infrastructure in scope generally followed the geographical characteristics and/or transport needs/profile of specific Member States. For instance, one landlocked Member State excluded the sea shipping sub-sector. Finally, it is worth noting that CIP measures in 22 Member States have a wider sectoral scope than that of the Directive, and consider sectors such as banking and finance, healthcare, drinking water supply, and digital infrastructure to contain vital CI. The fact that different Member States made different determinations concerning the sub-sectoral scope in the process of transposing the Directive may depend on if the Member States approached the task on a sectoral or cross-sectoral basis.

3.3 Identification of ECI

There is evidence of different starting points and approaches concerning the identification of potential ECI, which involves a four-step process described in the Directive. While some Member States already had a list of designated national CI prior to the adoption of the Directive, others viewed saw the adoption of the Directive as an opportunity to list existing infrastructure located on their territory for the first time. Specific findings regarding how the Member States approached the different stages of the identification process are presented below:

- In considering the first step of the identification process (the application of sectoral criteria), all Member States for which data was available (25 in total) apply sectoral criteria as indicated in the Directive;

- The second step (the application of the definition of CI), has been, generally speaking, transposed verbatim in national transposition legislation. The thresholds for the cross-cutting criteria described in the Directive are typically defined on a case-by-case basis and are confidential. Nevertheless, the evaluation found that the cross-cutting criteria are interpreted and implemented in many different ways across Member States, suggesting that the thresholds themselves can vary significantly, making cross-border comparison difficult. Furthermore, the process stipulates that 'for infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account'. The 'availability of alternatives' specifically was interpreted differently by Member States due to divergent views concerning how the notion of 'alternatives 'to disrupted/destroyed CI should be understood;

- The third step (the application of the transboundary element of the definition of ECI22) was transposed in similar fashion across the Member States, which typically re-stated the definition of European critical infrastructure provided in the Directive without providing any additional detail;

- The final step in the ECI designation process calls for each Member State to apply the cross-cutting criteria to any potential ECIs still under consideration. These cross-cutting criteria shall take into account the severity of impact and, for infrastructure providing an essential service, the availability of alternatives and the duration of disruption/recovery. The identities of any CI that meet these criteria are then communicated to other Member States deemed to be significantly affected in the event of disruption/destruction.

While it appears that the identification process was initiated by all Member States, only a limited number (11) ultimately identified at least one potential ECI in dialogue with neighbouring Member States. In most cases, those CI that were initially identified at national level did not pass through every stage of the four-step process, meaning that they were not assessed to be CI that could potentially be designated as ECI.

3.4 Designation of ECI

Aside from the requirement to designate a responsible competent authority (often indicated in national transposition legislation), the process of cross-border designation of ECI tends to be less formalised than the identification process. For instance, Member States typically do not specify how bilateral/multilateral discussions on designation should take place. This can be attributed to the fact that such discussions pertain to traditionally sensitive policy areas (e.g. national security, inter-state diplomacy). Nevertheless, the information that was provided by the Member States as part of the evaluation suggests that the discussions that take place as part of the designation process are conducted through different channels and with different degrees of formality (e.g. formal meetings/visits, exchanges of emails/informal letters, formal letters, working groups, telephone calls).

The final step in the designation procedure (informing CI operators that they have been designated as ECI) is often described in some detail in national transposition legislation, which typically stipulates the maximum amount of time permitted between designation and notification of operators, the form that this notification should take, and, in at least one case, by what means said notification should be communicated.

Around half of the Member States (six) that launched the designation process ended up with the designation of all, most, or half of the total number of potential ECI that were identified during the identification phase.

As of August 2018, the Member States had designated 93 ECIs, the identities of which are not public information. Of these, 88 were in the energy sector, with the remaining five in the transport sector. There is a strong geographical component to the distribution of ECI, with almost all designations in Member States in Central and Eastern Europe (with approximately 60% of the total number of designations in just two Member States).

It could be argued that, since the Directive has a focus on transboundary externalities and on the concept of 'affected Member States', Member States with long and/or a comparatively large number of shared borders may have engaged/been engaged in more bilateral ECI designation discussions than Member States with shorter borders and/or fewer immediate Member State neighbours. Geographical considerations may also explain a higher number of designations in Member States with a strategic position within the Union in terms of energy transmission, or in relation to energy distribution networks linking the EU with third countries.

Moreover, there appears to be a correlation between the number of designated ECI in different Member States and the type of transposition measures that were adopted at national level. For instance, the Member States that opted to embed the ECI identification and designation process within a wider CIP framework by means of legislative measures were more likely to have designated ECI on their territory. On the other hand, none of the Member States that chose to transpose the Directive through ECI-specific legislation/regulation ultimately designated any ECI. The same is true of most Member States that took administrative measures in implementing the Directive. In view of this finding, it would appear that norms relating to the identification and designation of ECI must 'find a place 'within a broader national CIP context in order for the ECI identification/designation process to go forward. Where this process is addressed within the context of sectoral legislation or isolated within ad hoc transposition norms, the likelihood for an ultimately successful ECI designation process decreases significantly

3.5 Specific Provisions in the Directive

The Directive contains a number of specific provisions that were addressed in-depth as part of the study. Among other things, the Directive requires that designated ECI have both an Operator Security Plan (OSP) and a Security Liaison Officer (SLO) function. In addition, the Member States are required to report certain types of information to the Commission on a regular basis, and to nominate a European CIP (ECIP) contact point.

3.5.1 Operator Security Plan (OSP)

The description of the OSP requirement in the Directive is very general. In some Member States, national transposition legislation stipulates that the content of the OSP must include the same level of detail as that provided by the Directive, while other Member States have imposed no such requirement. Like the identity of individual ECIs, the Commission does not have access to information concerning the content of ECI-specific OSPs; this is confidential information that was not made available during the evaluation and thus made comparison between OSPs impossible. Nevertheless, the evidence that was gathered during the field research phase of the evaluation via the CIP PoCs and CI owners/operators in the context of online and workshop-based consultations was sufficient to confirm that each Member State adopted the OSP provision using their own individual interpretations as to what needed to be done in light of what was already being done. In many cases, Member States had a pre-existing OSP-equivalent requirement in place at the time that the Directive was adopted. Rather than harmonise the OSP requirement across the Member States, the Directive in many instances simply served to formalise and bring under a legal framework efforts that were already being made at an operational level.

The Directive recommends performing OSP reviews on a regular basis. Only nine Member States indicated in their respective transposition legislation when reviews should be carried out. The remaining Member States for which data was available (11) required only that it is carried out regularly without indicating any specific time interval. The Member States opted for one of two general approaches in verifying that designated ECI owners/operators in fact have an OSP in place. The first, an enforcement approach, permits Member States to regularly conduct formal OSP reviews and spot checks, while the second involves close collaboration between government and operators (e.g. through structured CIP forums, public-private partnership (PPP) arrangements). With the latter approach, formalised 'enforcement 'measures were not seen as being particularly necessary.

3.5.2 Security Liaison Officer (SLO)

Transposition measures at Member State level typically did not involve the articulation of specific SLO requirements (e.g. role, key responsibilities, security clearance). This could be because the Directive does not clearly define the SLO function. While some Member States set out stringent criteria, others simply restated in their transposition measures the wording contained in the Directive. Any more refined articulation of SLO requirements at national level is usually provided for in resolutions and/or administrative decisions. As a result, the competencies, responsibilities and backgrounds of the individuals that are assigned the SLO role vary significantly from one Member State to another (and potentially even from one ECI to another in one and the same Member State).

One of the SLO's primary responsibilities is to be a link between the ECI and the national competent authority. However, in the majority of Member States, there is no explicit indication as to how in practical terms communication between the ECI and the national government should take place. This might be due to the fact that such information is confidential, but also to a lack of procedures, especially in Member States that had not designated ECI as of September 2018.

3.5.3 Reporting

Article 7 of the Directive puts in place certain reporting requirements on Member States with designated ECI, i.e. to every two years provide the Commission with generic data summarising the types of risks, threats and vulnerabilities encountered in those sectors where an ECI has been designated. These risks, threats and vulnerabilities should be identified through a confidential threat assessment process carried out by the Member States. The evaluation finds that these national threat assessments are typically focused on sector-specific issues and risks, and may include proposals for the implementation of organisational and technical measures aimed at building capacities to prevent, react to, and mitigate the possible consequences of different threat scenarios.

As for the biannual report on risks, threats and vulnerabilities to the Commission, a large majority of Member States adopted this provision at national level without making any further specifications; most Member States have simply identified the competent body (typically the CIP PoC/coordinating ministry) responsible for sending the necessary documentation to the Commission on a regular basis.

All Member States that designated at least one ECI submitted these reports to the Commission. However, the information contained in these reports was limited, making it difficult for the Commission to generate an overview at EU level concerning, for instance, threats/risks to CI. Without such information, it is difficult to synthesize the situational pictures at the Member State level in order to draw conclusions concerning CI vulnerabilities on a pan-European basis. For this reason, these reports have been of limited utility to the Commission.

Article 7 also stipulates that the Commission and Member States shall assess on a sectoral basis whether further protection measures at Community level should be considered for ECIs. This process was undertaken in conjunction with the 2012 review of the Directive, and fed into the formulation of a new approach to the implementation of the Programme emphasising the interdependencies existing between CI in different sectors. This involved the launch of four pilot studies examining different examples CI with a European dimension through which tools for risk assessment and risk management were developed. Furthermore, the Directive stipulated that common methodological guidelines for carrying out risk analyses in respect to ECIs could be developed by the Commission in cooperation with the Member States. This work was headed up by the Joint Research Centre (JRC) and resulted in a number of methodological support tools that were offered to the Member States for use on a voluntary basis.

3.5.4 European CIP (ECIP) Contact Point

Article 10 of the Directive stipulates that each Member State should designate a European CIP (ECIP) contact point charged with coordinating all issues concerning the protection of ECI at national and international level. This includes managing relations and interactions with other Member States and the Commission. The Directive leaves room for each Member State to allow other competent authorities, in addition to the one officially identified as the ECIP contact point, to be involved in CIP-related issues.

It is worth noting that a similar such function (a 'CIP contact point who would coordinate CIP issues within the Member State and with other Member States') was created in 2006 as part of the Programme. In practice, the ECIP contact points (required by the Directive) and the CIP contact points (recommended by the Programme) have de facto been merged into what is currently referred to as the CIP point-of-contact (CIP PoC), which has responsibilities concerning both CIP- and ECI-related issues.

The contact point functions 'institutional situation varies across the EU. While many Member States have designated CIP PoCs within the ministry of interior, others are organised within offices of the prime minister, ministries of defence, dedicated CIP or civil protection agencies, or sectoral regulators/oversight authorities. Given the range of entities with responsibility for nominating CIP PoCs, there is considerable variation in the level of specialisation of the CIP PoCs. While some CIP PoCs represent agencies or directorates within the competent ministries focused solely/primarily on CIP, others come from bodies that deal with a wide spectrum of matters of which CIP is one.

3.6 Organisational Arrangements at Member State Level

In order to fully appreciate the role of the CIP PoCs, it is important to acknowledge that the national-level organisational arrangements that have been put in place in order to implement the Directive (i.e. through the identification and designation of ECI, fulfilling specific obligations, reporting, etc.) vary significantly from one Member State to another in terms of both type and number of actors involved, as the figure below illustrates.

(...)

Depending on the Member State, the ECI identification process is initiated by different types of stakeholders, though sectoral ministries and regulators are clearly most typical (in 23 Member States). In most instances, these bodies act in coordination with a central authority (typically the ministry of interior). The type of authority that is responsible for ECI identification depends on the type of transposition strategy adopted by the Member States. For instance, the responsible authority tends to be a sectoral ministry/regulator in cases where transposition served to amend relevant sectoral legislation. Meanwhile, in cases where national-level transposition involves ECI-specific legislation, the use of inter-ministerial working groups is more common.

While there is considerable variation as to how Member States organise the work of identifying potential ECI, the outcomes of the external suggest that the ECI designation process tends to be elevated to the highest political level, and in some cases involves collective government decision-making. Elsewhere, designation decisions are made by the relevant sectoral ministry and/or the ministry of interior. There is considerable heterogeneity concerning responsibility for reporting to the Commission and conducting threat assessments, though in most cases (18 Member States) there is strong involvement by sectoral ministries.

The range of actors involved in implementing key elements of the Directive illustrates the extent to which national-level work pertaining to the Directive is fragmented. Indeed, the evaluation shows that the ECI identification and designation process and the fulfilment of related obligations (e.g. reporting, participation in CIP PoC-related activities) involve an average of three actors per Member State, as the figure below demonstrates.

(...)

5. Analysis and Answers to the Evaluation Questions

Evaluation question: To what extent is the Directive relevant in view of current and future needs/challenges?

Main findings:

- The Directive appears to have partial relevance in view of recent technological, economic, social, policy/political and environmental developments, and the challenges they entail.

- The Directive continues to be relevant in the context of the EU's CIP policy approach, but does not reflect the new approach to the Programme (2013), which emphasises interdependencies and resilience thinking.

- The objectives of the Directive remain relevant considering that the threats to CI (from natural hazards, terrorism, cyberattacks, hybrid actions, insider threats, etc.) persist. However, there is room to clarify what the 'common approach 'described in the Directive entails in practical terms.

- The definitions and procedures contained in the Directive are generally relevant, but due to a lack of detail, are subject to different interpretations and means of implementation at Member State level.

- The limited sectoral scope of the Directive means that it does not fully account for growing cross-sectoral interdependencies.

- The Directive's relevance in relation to stakeholder needs is mixed. While the Directive provides CI owners/operators, Member States and the Commission with an overarching framework for CIP, the generality of definitions and procedures leaves room for different degrees/forms of implementation that have the potential to generate costs.

By comparing the baseline situation (described in Section 2.4.2) with the implementation state of play (described in Section 3), it is possible to study to what extent the outputs and outcomes that can be observed (see the intervention logic in Section 2.4.1) correspond to the expectations concerning what the Directive should achieve, i.e. an increase in CIP capabilities in Europe and a reduction of CI vulnerabilities. The sections that follow describe the results of this analysis in relation to the six evaluation criteria, namely relevance, coherence, effectiveness, efficiency, EU added value and sustainability. (For an overview of the evaluation questions and sub-questions related to each criteria, see Annex IV.)

5.1 Relevance

The external study found that the increased interconnectedness of and interdependencies between sectors, along with the transboundary nature of threats and the potential cross-border consequences of the disruption/destruction of CI, demonstrate the continued need for the EU to be involved in CIP. This would seem to confirm the continued relevance of the concept of ECI, i.e. CI with particular pan-European significance and thus worthy of additional protective measures. While the specific objectives of the Directive (to create a procedure for the identification and designation of ECIs, and a common approach to the assessment of the need to improve the protection of such infrastructure) remain relevant, the Directive generally has only partial relevance. This finding takes into account the limited sectoral scope of the Directive, the definitions that it contains, how it has been implemented by the Member States, and its relevance to different stakeholders, including Member States and (E)CI owners/operators. This finding also accounts for and reflects the many technological, economic, social, policy/political and environmental developments that have taken place since the Directive was adopted in 2008.

The Directive is one element of the EU's overall CIP approach, which is described in the European Programme for Critical Infrastructure Protection. However, the Directive does not reflect the new

approach to the implementation of the Programme adopted by the Commission in 2013, which, for instance, emphasised the need for greater recognition of cross-sectoral interdependencies (some of which are not necessarily confined to the energy and transport sectors) and resilience thinking in the context of CIP. The fact that the Directive has not kept pace with more recent policy developments such as this are significant in the context of assessing its current relevance at EU level.

At a general level, the definitions contained in the Directive ('critical infrastructure', 'European critical infrastructure') are relevant insofar as they provide a foundation for a common CIP framework and support the identification of both CI and ECI. On the one hand, these definitions can be adapted to particular CIP-related goals that are articulated in specific CI sectors. The flexibility of these definitions reflects the Directive itself, which gives the Member States a significant amount of leeway in how they implement its provisions. On the other hand, the evaluation finds that these definitions lack the detail necessary for implementation and, as a result, are subject to different interpretations at Member State level. This in turn has limited their ability to achieve the EU-wide 'common approach 'to ECI identification and designation that the Directive was intended to generate. The Directive does not define terms such as 'assets', 'systems', 'critical', and 'protection' [*sic.*]. A more thorough articulation of such terms might increase the likelihood that Member States conceive of them in similar ways. Finally, in focusing on 'CI located in Member States', the ECI definition fails to take into account CI that have a clear pan-European dimension and which provide an EU-wide service (e.g. Eurocontrol, Galileo). This and all subsequent findings on relevance in this section were supported through the interviews, surveys and workshops that the external contractor carried out with Member States, CI owners/operators and other relevant stakeholders as part of the external study.

(...)

The narrow scope of the Directive, which is limited to the energy and transport sectors, does not fully account for the nature and extent of the cross-sectoral interdependencies that currently exist as compared to when the Directive was adopted. For instance, CI operations increasingly rely on services offered by the information and communications technology (ICT) and space sectors, though neither sector is covered by the Directive.

The 'means of implementation 'called for in the Directive include: the identification and designation of ECI and the relevant criteria; the development of an Operator Security Plan (OSP) for each ECI; the designation of a Security Liaison Officer (SLO) for each ECI; and regular reporting requirements. The evaluation finds that the descriptions of these implementation measures is very general, and is not well aligned with arrangements and practice at Member State level. For instance, the bilateral and/or multilateral discussion format initiated by one Member State to designate an ECI was found to inadequately represent the most relevant configuration for discussing cross-border CI issues, given that it does not make explicit provisions for private sector involvement, for instance. Furthermore, the descriptions of the OSP and SLO requirements lack detail, thereby limiting their relevance from an operational perspective. For instance, while the Directive makes clear that an OSP or 'equivalent measures 'should be put in place for each ECI and provides a general description of its content in an accompanying annex, it does not include any specific requirements as to content or what 'equivalent measures 'might entail. In any case, this issue is largely moot, as most designated ECI owners/operators already had security plans in place that they considered to OSP equivalents.

Finally, the Directive stipulates that all Member States with ECI provide regular reports on risks, threats and vulnerabilities for the designated ECI sectors to the Commission. However, the data that the Commission receives is limited, meaning that it is difficult to generate an overview at EU level on threats and risks. Without such an overview, it is difficult to assess the effects of the Directive and other EU policy initiatives on the protection of ECI, let alone the possible need for additional EU action in this respect.

The Directive's relevance in relation to stakeholders 'needs is mixed. While the external study found that the Directive provides CI owners/operators, Member States and the Commission with an overarching framework for CIP, it currently leaves room for differences in application that have the potential to generate different costs for different stakeholders in different Member States. (For a related discussion on costs in the context of effectiveness, see Section 5.2 below). For instance, the exact nature of the OSP requirements imposed by competent national authorities on ECI owners/operators may vary from one Member State to another.

The Directive lacks relevance insofar as it does not address the need for certain Member States to have exchange with third countries. This need was found to be most apparent in the case of Member States with immediate cross-border interdependencies with CI in neighbouring non-EU third countries. In a related vein, the external study found that the Directive has limited relevance in facilitating engagement with non-state stakeholders in the process of identifying and designating ECI. As mentioned earlier, there are no provisions in the Directive for private CI owners/operators to feed into the work of identifying ECI, be it in the host country or in a neighbouring Member State.

While none of the provisions contained in the Directive are considered altogether obsolete, certain definitions and the description of some means of implementation (i.e. the ECI identification/designation process, the OSP, the SLO function, reporting) could be more specific and better articulated. Furthermore, the relevance of the ECI concept in relation to the Member States 'conceptualisations of national CI (some of which are presumably also designated ECI) could be improved. Finally, the Directive might better account for other types of requirements that designated ECIs are subject to, including other EU measures, international guidelines/standards, and national initiatives, but also voluntary actions on the part of CI operators themselves.

5.2 Coherence

Evaluation question: To what extent is the Directive coherent and complementary to other relevant policy interventions at Member States, EU, and international level?

Main findings:

- The Directive appears to be broadly consistent with relevant sectoral legislation, with no conflicting objectives or obligations. However, its coherence is limited by the existence of certain overlaps with other pieces of European legislation/policy initiatives.

- At the EU level, the Directive is partially coherent but overlaps with the main policy interventions in the energy and transport sectors that are relevant in a CIP context.

- There are complementarities and to a certain extent overlaps between the ECI Directive and the Network and Information Security (NIS) Directive.

- The observed overlaps between different pieces of EU legislation do not appear to be particularly onerous on the part of public authorities and CI owners/operators at Member State level.

- At the international level, there is no comprehensive policy on CIP, though there are international standards and initiatives that apply to CI. Generally speaking, the Directive is coherent with these.

- There is room for better exploitation of the synergies that exist between the Directive and other sectoral initiatives and cross-sectoral initiatives at EU level.

The Directive appears to be broadly consistent with relevant sectoral legislation in the energy and transport sectors. However, the existence of several overlaps with these and other pieces of legislation as well as related policy documents limits the ECI Directive's coherence to some extent. While acknowledging that it has not been possible to determine conclusively whether these overlaps resulted in duplications or instead served to mutually reinforce one another, their very

existence suggests that there is room to streamline the EU's overarching CIP legislative framework.

At EU level, the Directive is partially coherent with the main CIP policy interventions in the energy and transport sectors insofar as they are partially complementary but also overlap in certain ways. The overlaps that have been identified by the external contractor pertain to things such as objectives, the object to be protected, as well as specific requirements (e.g. regular threat/risk assessments/analyses, risk management capability, incident response capability). With regard to the energy sector specifically, the Directive partially complements with and overlaps the relevant European legislation, and particularly in relation to what they aim to achieve (their stated objectives). For instance, the external study found that the objectives of the ECI Directive are complementary to those of energy sectoral legislation (insofar as the ECI Directive is focused on ECI protection while the energy sectoral legislation aims to ensure resilience in the face of disruptions). However, the external contractor found that the respective protective and resilience-oriented objectives of these measures were not clear-cut, leading to a risk for overlaps. The extent of overlaps appears to be more significant in the case of legislation in the transport sector, and especially in the aviation and maritime sub-sectors, and to some degree concerning measures on rail safety and security as well.

The evaluation also revealed complementarities and to some extent overlaps between the ECI Directive and the Network and Information Security (NIS) Directive (2016/1148) in terms of both objectives and objects to be protected. The objective of the ECI Directive is to improve the protection of ECIs defined as assets or systems. The NIS Directive aims to ensure the security of network and information systems on which operators depend for the provision of essential services. [emphasis added] The NIS Directive applies to seven sectors where operators of essential services meeting certain criteria shall be identified. These sectors include: transport; energy; banking; financial market infrastructure; health; drinking water supply and distribution; and digital infrastructure. The evaluation finds that the two Directives are complementary insofar as the ECI Directive acts to enhance the protection of systems and assets that are not ICT- based. On the other hand, the NIS Directive overlaps with the ECI Directive in any instances where designated ECIs in the transport and/or energy sectors depend on network and information systems for the provision of essential services. [emphasis added]

The external study was useful in depicting how different Member States and groups of Member States approach CIP and how these different approaches affect the implementation of the Directive at national level (see Section 2 and Section 3). At the national level, evidence provided by the Member States 'CIP PoCs and in carrying out the four case studies suggests that the observed similarities and, in some cases, overlaps between different pieces of relevant EU legislation did not generate significant duplications of effort or confusion on the part of public authorities and CI owners/operators. This was the case regardless of national CIP approaches and arrangements, which, as discussed earlier, vary from one Member State to another. This might be because the Directive defines obligations in general terms making them easily adaptable in different national contexts. That being said, the fact that national authorities have created mechanisms in order to deal with CIP in different sectors enables them to more systematically analyse and account for any overlaps that they might perceive to exist between different EU initiatives. For these reasons, the evaluation finds that the Directive is coherent with national CIP policy interventions in the energy and transport sectors. While the evaluation clearly demonstrates the ways in which the ECI and NIS Directives complement one another but also overlap, it is too early to assess how the inter-relationship between the two related measures has been dealt with by the Member States as part of the NIS transposition process (the deadline for which was May 2018).

With regard to more operational aspects of the Directive, the evaluation found that both the risk management measures included in the OSP and the threat assessment/risk analysis to be carried out by national authorities overlap with sectoral EU legislation. For instance, obligations on

operators to draft an OSP including a risk analysis and to define risk management measures are very similar to specific measures contained in aviation, maritime, and rail safety legislation, as well as rail security measures and the NIS Directive. Furthermore, the obligation imposed by the ECI Directive on national authorities to conduct a threat assessment/risk analysis mirrors similar obligations contained in European energy, aviation, maritime, and rail security legislation as well as with obligations contained in the NIS Directive.

At the international level, there is no single comprehensive policy on CIP. That being said, there are a number of international initiatives and standards that are directly or indirectly relevant in a CIP context. Generally speaking, the Directive is coherent with these insofar as it emphasises the same general challenges (e.g. a range of natural and man-made accidental and antagonistic threats, deep interdependencies between and among CI in different sectors) and puts forward similar policy prescriptions (e.g. transboundary/cross-border cooperation, the development of specific preparedness capacities, risk/threat analysis/assessment mechanisms). However, there are also cases of overlap, for instance between the Directive and various Recommendations put forward by the Organisation for Economic Co-operation and Development (OECD).

The EU's legislative framework on CIP, which consists of the Directive and other sectoral legislation with CIP relevance, appears to be coherent based on the findings of the external study. However, as noted above, certain similarities and, in some cases, overlaps have been identified. For instance, the ECI Directive overlaps with or is at least very similar to various energy sectoral initiatives as regards their stated objectives, the object that should be protected, and the requirements for threat assessment/risk analysis. The situation is similar with regard to aviation, maritime and rail initiatives in the transport sector, and in relation to the NIS Directive. This suggests that there is room for better exploitation of the synergies that exist between the Directive, specific sectoral initiatives, and cross-sectoral initiatives like the NIS Directive. Generally speaking, the Directive complements other initiatives, and few overlaps can be found in relation to the specific obligations on Member State authorities and ECI owners/operators imposed by the Directive. That being said, the Directive tends to be managed in parallel with other CIP-relevant initiatives that have been taken since 2008. This is true, for instance, in the context of the Union's work on the countering the hybrid threat and with regard to the space sector, where the obligation concerning protection for the ground component of Galileo currently presupposes that it is treated as ECI at national level. The external study finds that examples such as this point to the need for a more closely aligned and holistic CIP approach at EU level in order to encourage better coordination of all CIP-relevant activities and to mitigate against the risk for misalignments between and among different distinct but related work streams that in one way or another serve to enhance CI protection and resilience.

Limited integration between CIP measures at EU level does not seem to be reflected at the national level according to a considerable majority of CIP PoCs (89%) that responded to an online survey as part of the external study. At national level, protection measures applied in different sectors co-exist and are coordinated in ways that contribute to the overall coherence of national CIP frameworks and reduce the likelihood for duplication. As mentioned elsewhere, this may be explained by both the ability of Member States to account for the similarities and overlaps that exist between different measures, but also the generality of the obligations deriving from the ECI Directive specifically.

5.3 Effectiveness

Evaluation question: To what extent has the Directive been effective in delivering intended results?

Main findings:

- The Directive has been partially effective in achieving its stated objective, i.e. the establishment of a common ECI identification and designation procedure. While the Directive introduced

elements of a common CIP framework and established a procedure for the identification/designation of ECI, it has not succeeded in ensuring that these are fully aligned across all Member States.

- Internal and external obstacles to the implementation of the Directive impacted the progress towards achieving its objectives. For instance, in many Member States, the Directive had to find its place within national CIP frameworks that were already partially or fully formed, thereby limiting the uptake of the Directive.

- The Directive generated effects that went beyond its intended objectives, i.e. spill-over effects in the CIP realm.

The Commission sought to address an inadequate level of protection of CIs with a European dimension in the energy and transport sectors against natural disasters, technological threats, and man-made threats, including terrorism, when it put forward its proposal for an ECI Directive. As it was adopted, the Directive aimed to address this problem through the establishment of a procedure for the identification and designation of ECIs and a common approach to the assessment of the need to improve the protection of ECIs (the two specific objectives of the Directive according to the intervention logic presented in Section 2.4.1 of the external study).

The Directive included a number of provisions (or inputs) which were to be used to achieve its stated objectives. These provisions provided the Member States with common definitions that would enable them to more easily carry out discussions over Member State lines with the aim of jointly identifying CIs with potentially serious cross-border implications if disrupted in one way or another. These same Member States would then jointly designate CIs with 'European ' implications and take additional mandated protective measures (i.e. the development of OSPs and designation of SLOs). The Directive also contained provisions allowing the Commission to support ECI owners/operators as necessary, to stimulate EU-wide exchange on CIP-relevant issues (through the points-of-contact group), and to maintain a general overview of the threats, risks and vulnerabilities facing specific sectors in which CIs with European implications operated through regular reporting by the Member States.

The evaluation finds that the Directive has been somewhat effective in achieving its stated general and specific objectives through the provisions described above and in Section 2.4.1. This can in part be explained by the fact that some of the provisions contained in the Directive have been only partially achieved. For instance, the relevant definitions contained in the Directive (e.g. 'critical infrastructure', 'assets', 'systems') are vaguely formulated, thereby leaving room for different interpretations and limiting the Directive's harmonising power. Furthermore, the external study found that, on the basis of responses by Member States and CI owners/operators and the outcomes of the case studies, while the Directive includes a common procedure for the identification and designation of ECI, the contours of the procedure vary from one Member State to another. In other words, the procedure is by no means common or harmonised across the Union.

In other respects, however, the Directive has achieved progress in relation to the stated objectives, though this has been limited by certain factors and circumstances. For instance, the Directive stipulates that all Member States with designated ECI provide regular reports on risks, threats and vulnerabilities for the designated ECI sectors to the Commission. However, the generality of the common reporting template that Member States should use, combined with reluctance of the Member States to share sensitive information, has limited the utility of the reports that are submitted. Were the content of the reporting provided by the Member States more elaborated, it might be used by the Commission to gain a more precise understanding of the threats, risks and vulnerabilities facing ECIs across the Union, which could be useful both for the Commission and individual Member States.

The Directive also imposes OSP and SLO requirements on ECI owners/operators. However, ECI owners/operators in most Member States already had SLO- and/or OSP-equivalent measures in place prior to the adoption of the Directive. As such, the impact of the Directive vis-à-vis this specific output has been mainly in formalizing already existing measures.

Finally, the Commission has offered various forms of support to CI owners/operators in helping them fulfil the Directive's provisions. Examples include the facilitation of cooperation, the sharing of good practices and methodologies (some of which were developed by the JRC), training, and funding through, for instance, the EU Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks (CIPS). Meanwhile, delegates to the points-of-contact group stipulated in the Directive have been designated by the Member States and meet on an approximately twice-yearly basis.

However, the full achievement of the Directive's general objective has been hampered by certain obstacles, some of which are related to the design of the Directive itself, while others are of an external nature. For instance, the Directive does not include a monitoring and evaluation framework that could be used by the Commission in order to effectively track its implementation by the Member States (even in absence of information concerning the identities of specific ECIs). Furthermore, there is currently no dedicated funding associated with the Directive that could be used to support competent authorities or CI owners/operators (though EU funding for various kinds of CIP programmes, projects and workshops was available before the Directive was adopted (e.g. starting in 2007 through CIPS). Funding has since been made available through the Internal Security Fund (ISF) as part of the current Multiannual Financial Framework (MFF) and the Horizon 2020 research programme. In every instance, efforts have been made to share the results of funded projects and studies via the Critical Infrastructure Warning Information Network (CIWIN) and in the context of regular meetings of the CIP PoCs.

Other obstacles are external to the Directive. In almost half of the Member States, the Directive had to find its place within national CIP frameworks that were already partially or fully formed. In some instances, this served to limit the extent to which Member States availed themselves of some of the voluntary provisions contained in the Directive. One explanation that the external study provides is that in many cases existing national mechanisms/programmes could be used to support the implementation of the Directive on the part of designated ECIs. On the other hand, a substantial number of Member States lacked fully-fledged CIP frameworks prior to the adoption of the Directive. In such cases, the Directive proved, generally speaking, to be a catalysing factor in designating ECI. Even so, this has not led to a wide-ranging effort across the Union to identify and designate ECIs. As an example, almost half of the Member States that lacked well-developed CIP frameworks prior to 2008 have yet to designate any ECI. This might suggest that enthusiasm for EU action in this policy area was lacking in some Member States, and, where this was the case, served to limit the implementation of the Directive. Finally, the reluctance of Member States to share sensitive information has created challenges for the Commission in monitoring the implementation of the Directive. As such, the Commission has limited access to indicators beyond how many ECI per Member State have been designated. This makes it difficult if not impossible for the Commission to see whether and how the Member States have in fact complied with the Directive's provisions, let alone if the Directive has led to an increase in the protection of designated ECIs.

Despite the obstacles to implementation described above, the Directive has been found to be effective in generating spill-over effects beyond its intended objectives. For instance, according to a majority of the CIP PoCs (65%) who were surveyed as part of the external study, the Directive generated awareness of and political momentum around the protection of CI in general, and not just in relation to ECI in the energy and transport sectors. Furthermore, in the case of Member States that either had no pre-existing CIP framework or where the existing framework was only partially developed prior to 2008, the Directive spurred efforts aimed at creating dedicated

national-level CIP legislation, common national definitions of critical infrastructure, and/or obligations to carry out threat assessments.

Finally, in considering the overall impact of the Directive in improving the level of protection of CI with EU relevance (the Directive's primary aim), the results of the evaluation are inconclusive. On one hand, the creation and/or further strengthening of national CIP frameworks in half of the Member States, as well as similarities between European and national requirements concerning the protection of ECI and CI, respectively, seems to suggest that CI with European relevance are protected equally, no matter if they are designated as ECI or not. On the other hand, the available evidence demonstrates that national requirements for both CI and ECI protection vary from one Member State to another (and perhaps even from one ECI owner/operator to another). Therefore, the possibility that actual levels of protection vary as well cannot be excluded. An in-depth assessment of the measures included in the OSPs used by individual ECIs (the identities of which are not known) would be needed in order to generate more insights on this and other related questions.

5.4 Efficiency

Evaluation question: To what extent has the Directive achieved intended results in the most efficient manner?

Main findings:

- While there is no conclusive evidence that the results attributed to the Directive have been achieved at a reasonable cost, the scale of the costs brought about by the Directive appears to be limited.

- The lack of quantifiable data prevents making a sound assessment of the regulatory burden brought by the Directive.

- The overall efficiency of the Directive has been limited by a number of factors, many of which stem from the generality of the Directive's provisions.

Due to the sensitivities associated with CIP generally and ECI designations specifically, the external contractor had only partial access to relevant empirical data in carrying out the analysis of the Directive's efficiency. This made it impossible to definitively quantify the costs incurred as a result of the Directive. Moreover, as Member States are not obligated to communicate the identities of ECIs, it was not possible to distinguish between operators of national CI and ECI. This made the analysis of specifically the costs associated with Directive implementation complex. Due to a lack of certain types of data, the external study was focused on gauging the incidence of these costs in those Member States that might be affected by the specific obligations introduced by the Directive. This was used as a proxy for assessing the scale of the costs that can be attributed to the Directive under the assumption that the higher the number of obligations involving significant costs, the wider the scale of the overall costs incurred on account of the Directive.

There is no conclusive evidence that the results attributed to the Directive have been achieved at a reasonable cost. The introduction of the Directive put in place a set of obligations for Member State authorities and ECI owners/operators to meet. For instance, competent national authorities were obligated to identify and, where appropriate, designate ECI within their jurisdictions, while ECI owners/operators were required to develop OSPs and designate SLOs (or equivalents). Fulfilling these obligations entailed certain compliance and administrative costs for both competent Member State authorities and CI operators/owners, and, to a lesser extent, enforcement costs for competent authorities.

The scale of the costs brought about on account of the Directive appears to be limited. Firstly, incurred costs seem to have had a limited incidence. This is due to the fact that most of the obligations introduced by the Directive (e.g. the OSP and SLO functions) were already in place in several Member States. Furthermore, specific pieces of sectoral legislation contain similar

requirements that had already been met by the affected stakeholders. Likewise, the requirement to designate contact points had de facto already been met by the Member States as part of the implementation of the Programme launched in 2006. For these reasons, the only new costs incurred as a result of the Directive were in relation to the obligation to inform the Commission about the designation of ECI and then provide regular reporting.

Most of the costs associated with implementation are only incurred once an ECI has been formally designated, which only occurred in a limited number of cases in a relatively small number of Member States. The competent authorities at Member State level and CI owners/operators that were consulted as part of the external study tended to agree on the fact that the costs associated with designation (e.g. development of an OSP, designation of an SLO, regular reporting) represented a minor share of the overall budget allocated to the protection of CI. In other words, the costs brought about by the Directive, and the fact that only a limited number of Member States had to bear most of them appears to be proportionate to the limited results achieved by the Directive. That being said, the lack of quantifiable data concerning actual costs incurred by specific Member States concerning specific ECIs made it difficult to make a sound assessment of the regulatory burden brought about on account of the Directive.

Besides questions of cost, a number of other factors also affected the overall efficiency of the Directive. Some of these factors stem from or are inherently related to the scope and design of the Directive itself while others are external to it. For instance, the generality of the provisions contained in the Directive allowed Member States to adapt existing national approaches without needing to create completely new procedures. At the same time, these choices at the national level created additional costs for operators that varied from one Member State to another. Additional limiting factors included: differences in how the OSP was operationalised on the part of ECI owners/operators in different Member States; fragmentation in the organisational arrangement of CIP policy (making it difficult for Member States to identify counterparts to discuss ECI identification and designation on a cross-border basis); and differences in national data protection and privacy laws.

5.5 EU Added Value

Evaluation question: To what extent has the Directive achieved EU added value as opposed to what could have been achieved at either the national or the international level?

Main findings:

- The Directive generated some EU added value insofar as it achieved results that national or other EU initiatives would not otherwise have achieved. Where national or other EU initiatives might have been able to achieve the same or at least similar results, this would only have been achieved through longer, costlier and less well-articulated processes.

- The Directive created political momentum at both European and national level concerning CIP. The Directive also served to underscore the fact that CIP was a priority at EU level.

- The Directive paved the way for the creation of a common framework for the protection of ECI, and provided a common vocabulary. However, the potential EU added value that could be derived from this achievement was limited by considerable heterogeneity in how different Member States interpreted the Directive's provisions.

- The perceived EU added value of the Directive, especially in contributing to the creation of a common European ECI identification and designation framework, varies from one Member State to the next. Specifically, the OSP, SLO and reporting requirements generated limited EU added value due to the fact that the Directive provided insufficient detail concerning their contents.

- The Directive triggered cross-border dialogue and operational co-operation in a field (CIP) that was considered to be the exclusive competence of the Member States prior to 2008.

The evaluation found that the Directive generated some EU added value insofar as it achieved results that national or other EU initiatives would not otherwise have achieved. It also created value in producing results that national or other EU initiatives could arguably have achieved in the absence of the Directive, albeit through longer, costlier and less well-defined processes. This assessment is based both on the outcomes of the external study and certain conclusions presented earlier in this document (e.g. that the Directive is partially relevant in light of the current threat picture and policy landscape and somewhat effective in relation to its stated general and specific objectives).

Specifically, the Directive contributed EU added value by paving the way for the creation of a shared framework for the protection of ECI. In a context of highly diversified approaches to CIP and different degrees of national programme maturity, the Directive managed, for instance, to introduce a common European vocabulary, an essential step in facilitating effective cross-border dialogue on CIP-related issues. However, the potential EU added value that could be derived from this achievement was limited by the high degree of heterogeneity in how different Member States interpreted these definitions and the procedures provided by the Directive.

Moreover, the EU added value of the Directive, especially in terms of its contribution in creating a common framework, is perceived differently by different Member States. While some Member States saw in the Directive an opportunity to develop a more comprehensive CIP framework, others considered the Directive as being a weaker measure than the CIP frameworks that they already had in place. It is particularly in the latter case that Member States struggled to discern between the requirements of the Directive and pre-existing obligations at national level.

Practically speaking, the OSP, SLO and reporting requirements proved to have limited EU added value. For instance, the evaluation found the OSP and SLO functions to be under-developed in terms of detail, which made them difficult to apply in practice. Meanwhile, again, many Member States already obligated operators to take very similar measures, the contours for which were much better articulated. The EU added value related to the reporting obligation is limited by the fact that the reports submitted to the Commission typically lack the data necessary to generate an overview at EU level on threats and risks. Such information would arguably be useful in informing future policy decisions related to CIP.

The Directive acted as a catalyst for change by generating political momentum on matters related to CIP. This was reflected by both the CIP PoCs and CI owners/operators that were consulted via online surveys and in the context of several consultative workshops in Brussels. Specifically, the Directive served to convey the importance of CIP at EU level, and framed CIP in a wider EU context by giving considerable visibility to specific threats (e.g. terrorism) and stressing the importance of cooperation with operators and across borders. The need for transposition of the Directive ensured that CIP achieved new attention at national level as well. Some Member States that had limited or no CIP framework prior to 2008 introduced specific legislation on CIP; in at least one case, a dedicated national CIP agency was created. Meanwhile, the Directive prompted other Member States to make changes to pre-existing CIP practices, for instance by embracing an all-hazards approach over more threat-specific approaches. While such effects at national level could conceivably have been achieved through other pillars of the Programme, the existence of EU legislation on CIP arguably made implementing such changes easier. It also served to speed up national decision-making processes and to encourage cooperation between Member States (not least through the cross- border ECI identification and designation process and the creation of CIP national contact points).

The Directive also served to underscore the fact that CIP was a priority at EU level. Simply put, the Directive ‘elevated ’the discourse at the EU level, and made the argument that CI disruptions/failures in one Member States could have cross-border implications. This heightened interest in CIP trickled down to the national level both in those Member States where there were no or only partial CIP frameworks in place and in Member States where more robust CIP programmes already existed.

Moreover, the Directive triggered the creation of cross-border dialogue and operational cooperation in a field that had traditionally been viewed as the exclusive competence of the Member States. Numerous provisions in the Directive (e.g. the procedures for discussing cross-cutting criteria in the identification process, the appointment of CIP PoCs, the organisation of regular meetings) contributed to processes that created additional mutual understanding and trust between Member States (much of which was already being fostered through the Programme).

5.6 Sustainability

Evaluation question: Are the effects already achieved on account of the Directive likely to be long-lasting, if the Directive were repealed?

Main findings:

- Several effects generated by the Directive are likely to be long-lasting and would continue to exist in the event that the Directive was repealed and not replaced.

- On the other hand, some of the direct effects achieved by the implementation of the Directive would likely cease to be felt.

The Directive was part of a trust-building exercise that began with the Programme in 2006 and continued via a number of incremental steps. The Directive has been the impetus for a range of activities, many of which have become more consolidated over the years. At the same time, new initiatives, sectoral and more broad-based, have been developed. In the process, the effects of the Directive have become less reliant on the Directive itself.

Several effects generated by the Directive are likely to be long-lasting and would continue to exist in the event that the Directive was repealed and not replaced with another legislative instrument. For instance, certain spill-over effects brought about as a result of the Directive are likely to persist. These include, for instance, regular CIP PoC meetings, sectoral initiatives, discussions related to the implementation of the NIS Directive and various activities and programmes administered by the JRC, one example being the European Reference Network for Critical Infrastructure Protection (ERNCIP). Furthermore, many of the coordinative structures and entities (including at least one national CIP agency) that were created at national level in certain Member States in order to implement the ECI Directive could also be leveraged in implementing the 2016 NIS Directive. In one way or another, these spin-off effects provide different forms of platforms for discussion, cooperation, awareness- raising and continued trust-building on issues related to CIP. Some of the effects stemming from the implementation of the Directive on the part of the Member States and ECI owners/operators are now deeply rooted in national practices and not likely to be subject to significant change were the Directive to be repealed. However, other direct effects would likely cease to be felt. This might include certain forms of operational cooperation and exchange of information between Member States.

The negative effects resulting from a hypothetical repeal would likely outweigh any benefits. Repealing the Directive would send the signal that the protection of ECI is no longer an EU priority, and might engender actions at Member States level that could reduce the sustainability of the results achieved.

6. Conclusions

The overall objective of the external evaluation was to evaluate the implementation of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The evaluation considered the implementation of the Directive in light of six evaluation questions informed by criteria provided

in the Commission's Better Regulation Guidelines (relevance, coherence, effectiveness, efficiency, EU added value and sustainability).

The analytical framework that was developed in order to evaluate the Directive was able to overcome a number of limitations, including: an unclear pre-2008 baseline situation as a point of comparison; the limited availability of information concerning relevant national measures; not knowing the identities of designated ECIs; and challenges in distinguishing the effects of the Directive from other national- and European-level measures. The solutions that were devised in order to overcome these limitations ensured that the data that was collected from a wide range of consulted stakeholders was of sound quality and provided a solid basis from which to answer the evaluation questions.

On the basis of the comparison that was made between the baseline situation (described in Section 2), the implementation state of play (in Section 3), and feedback from stakeholders, the evaluation found that:

- The context in which CI are operated has changed considerably since the Directive entered into force. In view of recent technological, economic, social, policy/political and environmental developments and the new and evolving challenges that they pose in protecting CI, the Directive has partial relevance;

- The Directive appears to be broadly consistent with relevant European sectoral legislation as well as policy at international level. Several complementarities and overlaps with other pieces of European sectoral legislation/policy documents in the energy, transport and ICT sectors exist;

- The Directive has been partially effective in achieving its stated objectives, i.e. to improve the level of protection for ECIs in the energy and transport sectors by creating a common framework for the identification and designation of ECI. Meanwhile, because the generality of some of the Directive's provisions left room for different interpretations by Member States, it has only to a limited degree achieved the objective of establishing a common approach to the assessment of the need to improve the protection of ECI. That being said, the Directive has generated certain spill-over effects (e.g. increased awareness about CIP, political momentum, national-level legislations/definitions/obligations in Member States with no pre-existing CIP framework). The evaluation was ultimately inconclusive as to the contribution of the Directive to the overall objective of an improved level of protection of CI with EU relevance;

- The evaluation found no conclusive evidence that the results attributed to the Directive have been achieved at a reasonable cost. While the extent of the costs associated with implementation of the Directive appear to be limited, a lack of available quantifiable data from the Member States and ECI owners/operators makes it difficult to carry out a sound assessment of the Directive's regulatory burden on stakeholders; stakeholders 'views on the proportionality of the costs in relation to observable results is mixed. Besides certain incurred costs, a number of other factors have affected the overall efficiency of the Directive, some which stem from the nature and substance of the Directive itself (e.g. the generality of key provisions and definitions, the absence of a strong monitoring and evaluation framework) and others that are external to it (e.g. the existence/level of maturity of national-level CIP frameworks prior to the adoption of the Directive);

- The Directive generated EU added value insofar as it achieved results that national or other EU initiatives would not otherwise have achieved, or that national or other EU initiatives would have achieved anyway, albeit through longer, costlier and less well-defined processes. One example is a common framework for the protection of ECI (although different Member States interpret the 'commonality 'of this approach differently). On the other hand, certain specific provisions, like the Operator Security Plan, the Security Liaison Officer function and reporting requirements, proved to have limited added value for many Member States.

- Several effects generated by the Directive are likely to be long-lasting and would continue to exist in the event that the Directive was repealed and not replaced. On the other hand, some of the direct effects achieved through the implementation of the Directive (e.g. cross-border CIP discussions, reporting requirements) would likely cease to be felt.

The evaluation makes clear that the Directive, a central pillar of the European Programme for Critical Infrastructure Protection, initially played an important role in bringing attention to bear on CIP and, in the case of those Member States that were undertaking limited CIP activity at the time, sparked a considerable amount of new work aimed at enhancing critical infrastructure protection and resilience at national level. After the Directive's entry into force, an evolving threat picture involving a combination of natural and (sometimes antagonistic) man-made threats, but also the increasingly intertwined, transboundary and 'wired 'nature of Europe's critical infrastructure and the services that they together provide would gradually reduce the Directive's relevance. In many instances, the interdependencies between CIs in different sectors are considerable, extend beyond Europe's boundaries, and need to be accounted for in addressing the security of European CI in the years to come.

The preponderance of evidence collected during the evaluation indicates that while some elements of the Directive remain useful, others are of limited value today and could be revisited in order to better achieve the Directive's stated overall objective (an improved level of protection of ECIs in the energy and transport sectors). This could mean shifting the focus away from asset protection to one that is more systemic in nature and which recognises interdependencies across a range of different sectors (much like the NIS Directive does in the ICT realm). Meanwhile, the evaluation provides a reminder that many Member States have incorporated resilience thinking into their national CIP frameworks. This means ensuring that CI are both well protected and capable of quickly recovering from disruptions in those instances where protective measures are inadequate.

The consultations with stakeholders that were carried out as part of the evaluation suggest that there is continued support on the part of Member States for EU involvement in CIP policy. While opinions on the matter varied, the outright repeal of the Directive was seen by many Member States and CI owners/operators as likely to have negative effects. That being said, a number of Member States argued during the consultations that CIP is primarily a national responsibility and, as such, suggested that the EU's engagement both now and in future should respect the principle of subsidiarity and demonstrate clear EU added value, both in supporting Member States 'CIP work at national level and in facilitating cross-border cooperation, including with third countries outside the Union.

Based on the findings of the evaluation, there is clearly room for further reflection at EU level as to how best further improve the protection of CI in Europe, including the 93 ECIs that have been designated thus far. This should include focused consideration of how the EU can most effectively provide support to the Member States and CI owners/operators that host, oversee and/or run vital infrastructure. This conclusion has been borne out through discussions with the Member States, CI operators and operator associations, as well as other partners, including international organisations and third countries that have taken place in recent years, including in the context of the evaluation. The findings of the external study that informed the evaluation are in line with the Commission staff's own analysis concerning the Directive.

As mentioned earlier, closer alignment of the EU's CIP policy with the essential services approach described in the NIS Directive might better reflect how issues related to critical infrastructure protection and resilience are currently being addressed at Member State level. Further work would be needed in order to assess the potential advantages of aligning CIP and NIS policy so as to ensure enhanced complementarity between cyber and physical protection measures relating to CI in different sectors. Any such deeper analysis would necessarily explore how any further action might build on and strengthen ongoing work related to the implementation of the NIS Directive. However, going from an asset-focused CIP approach to one that is more systems-

focused in nature and that emphasises interdependencies between different CI in different sectors cannot be achieved using the Directive as it is articulated today.

The external study provides the Commission with a range of recommendations that could be useful in enhancing the utility of the Directive as it stands today. For instance, the study suggests that the Commission strengthen elements of the monitoring and evaluation framework, and maintain and make available to the Member States an overview of available EU funding and EU-funded CIP-relevant research/projects. While such recommendations could be acted on in relatively short order, others, like the suggestion to further develop key definitions and provisions or to extend the Directive's sectoral scope, would require more reflection informed by additional consultations with the Member States and other stakeholders in a wide range of sectors.

The consultations that were carried out during the evaluation reinforce the need for any further action on CIP to account for the far-reaching interdependencies that exist across many different sectors besides energy and transport. As this evaluation suggests and the NIS Directive demonstrates, there are additional sectors that the Member States consider worthy of additional protective action at European level. This is as much due to the important services that they provide individually as for the interdependencies that exist between them. While the 2013 revision of the Programme included a better accounting for CI interdependencies, the Directive itself was left unchanged. Based on the evaluation's findings, there are grounds to examine the scope of the EU's CIP policy framework to encompass additional sectors, and to develop strategies for identifying and addressing those vulnerabilities that result from the interdependencies that exist between them.

The study serves as a reminder that several legislative initiatives have been adopted since 2008, and that many of these overlap with the Directive in different ways. Any further action on EU-level CIP policy would need to be coherent with existing and foreseeable future legislation so as to increase its EU added value and to reduce the risk of undue burdens being placed on Member States and CI owners/operators. In this context, it is necessary to fully understand the relationships that exist between the ECI Directive and more recent pieces of legislation and other related measures on, for instance, security of energy supply.

Furthermore, the evaluation shows an evolution in the nature of the threats facing Europe, some of which are longstanding while others are either arguably new (like unmanned aerial vehicles or artificial intelligence) or evolving (insider threats). While the introduction of improved capabilities (like 5G) will improve efficiencies, they may also generate new or exacerbate existing vulnerabilities. Furthermore, the implications of third-country ownership/control of CI in Europe require careful monitoring. For these reasons, the EU's approach to CIP must be a flexible, risk-based one that corresponds to the spectrum of current and future threats and vulnerabilities facing Europe's critical infrastructures.

Finally, the Directive has not kept up with the Member States 'thinking on resilience, i.e. the ability for CI to recover quickly from adverse events, antagonistic or otherwise. Obviously, protection is an essential element to the defence of infrastructure (in its own right or as a generator of essential services). However, these measures go only so far in ensuring that CI that has been adversely affected by events is able to quickly bounce back in order to continue delivering the services that European society relies on for a certain quality of life. This again points to the need for further reflection on a more explicit resilience dimension to EU-level CIP policy that would support related ongoing work at Member State level, and at the same time bring it more closely in line with EU policy in the field of civil protection and security of supply, for instance.

ENISA publications

1.1 Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks (December 2014)

Executive summary

Communication networks are an important component of the life of millions of European citizens. These networks represent the fabric of the future information society and provide the means for the single digital market. Some parts of these communication networks are also vital for the operations of Critical Infrastructures which are fundamental for the function of modern society.

An attack or a large scale outage affecting the communication networks assets supporting Critical Infrastructure can have cascading effects and affect large part of the population or vital functions of society. But which are exactly those network assets that can be identified as Critical Information Infrastructure and how we can make sure they are secure and resilient?

This study aims to tackle the problem of identification of Critical Information Infrastructures in communication networks. The goal is to provide an overview of the current state of play in Europe and depict possible improvements in order to be ready for future threat landscapes and challenges. As it was possible to underline, currently a significant number of Member States present a low level of maturity and lack a structured approach regarding identification of Critical Information Infrastructure in communication networks and this can pose severe risks regarding the everyday increasing dependency of the vital functions of the society on these networks.

Moreover, based on the findings of the survey, the discussion with stakeholders and the analysis of the different approaches already in place, it was possible to highlight the following challenges in identifying CIIs assets and services:

- detailed list of critical services is not always present and should be tailored per Member State

- criticality criteria for the identification of critical assets is a challenging process especially regarding internal and external interdependencies

- effective collaboration between public sector and the private sector is fundamental in identifying and protecting CII assets and services and should start from asset identification.

Considering this multi-layered and complex environment and raising threat scenarios, the following recommendations emerged for Member State and operators of critical infrastructures to foster security and resilience of CIIs over communication networks in Europe:

Member States should clearly identify Critical Information Infrastructures if not already covered in their Critical Infrastructure activities. Not all MS have clearly defined the asset perimeter of Critical Information Infrastructures. For this reason, if not already covered by the Critical Infrastructure definition, Member states should clearly define which specific network assets are covered and should be secure and resilient.

Member States who are starting to work on the identification of CII assets should cooperate with stakeholders involved in the operations of Critical Information Infrastructures. Effective collaboration between public sector (Government & mandated Agencies) and the private sector is fundamental in protecting CII assets and services. For the identification of Critical Information Infrastructures in communication networks, the involvement of two categories of stakeholders should be pursued:

- operators of Critical Infrastructures

- network operators

given the complementarity of their perspectives, responsibilities and expertise.

Member States who are starting to work on the identification of CIIs should adopt a methodology for the identification of critical network assets and services, using one or a mix of the proposed solutions in this study that better fits the need of the MS. It is worth-noting that the purpose here is to present the Member States with a portfolio of methodological approaches – rather than a one size 'fits-all 'methodology – so that each Member State may choose the approach or a combination of approaches that suits better to its own specific characteristics and needs.

Member States who base their identification of CIIs on critical services should develop a list of these services and assess internal and external interdependencies. While assessing the criticality of services, infrastructures and supporting network assets, MS should define criticality criteria in order to identify the critical assets and examine the system in its entirety rather than per constituent. At least four types of dependencies should be taken into consideration:

- Interdependencies within a critical sector (intra-sector).

- Interdependencies between critical sectors (cross-sector).

- Interdependencies among data network assets.

Moreover dependencies can be found at the national and international level (cross-border), further complicating the task to have a complete overview.

Member States should foster baseline security guidelines for communication networks used for critical services. To ensure the resilience of critical networks, the Critical Infrastructure operator or asset owner should adopt security guidelines to be used also at procurement stage. For this reason a checklist with baseline security guidelines for communication networks used for critical services should be made available to align practices across the EU.

Member States should foster the adoption of automated procedures for CIIs tagging in order to be prepared to face future challenges. To foster the security of critical networks, MS should work together with CIIs asset owners in developing a common approach to the 'Tagging 'of CII assets. This could allow automated-prioritized handling of incidents affecting Critical Information infrastructures.

(…)

1.2 Stocktaking, Analysis and Recommendations on the Protection of CIIs (January 2016)

Executive Summary

The internet and other digital technologies as well as its underlying network and information systems are the backbone of the European Society and the Digital Single Market. Many critical sectors operating in the European Member States such as the energy, transportation or financial sectors rely on critical information infrastructure (CII). The Threats to CII, which stem from different sources ranging from national actors to criminal hackers, have increased in recent years. In order to fully meet the emerging threats to CII, ENISA offers assistance to EU Member States and the EU Commission.

This study contributes to the improvement of the protection of critical infrastructure in Member States by taking stock of and analysing existing measures deployed in the field across several EU Member States. The goal is to provide a set of good practices and recommendations to national authorities and lawmakers which will contribute to stronger and more resilient CII in EU Member States and decrease the risk of disruption or failure of critical infrastructure.

The introduction identifies six action areas for Member States, which contribute to an effective national protection of CII (CIIP). These action areas include comprehensive policies and legislations [*sic.*], but also effective national governance structures during day-to-day operations

and in cases of emergency. Information sharing between the private and the public sector and threat intelligence constitute important elements in CIIP, since critical information infrastructure is mainly owned by the private sector.

This study presents some key findings, uncovers the different governance structures for CIIP in seventeen EU Member States and one EFTA country along with different good practices. In addition, it presents general findings, based on collected information via interviews and online surveys:

- Surveyed EU Member States have delegated responsibility to cyber security authorities, emergency agencies or national regulators. Only a minority of the examined Member States have tasked intelligence agencies or information security forums with CIIP

- Almost all national authorities for CIIP are responsible for operational tasks (for example: PoC for incident reporting, organising exercises, incident response). Two thirds of the authorities are responsible for additional tasks on the strategic or political level, such as the development of strategy papers, supervision of the national CSIRT or the proposing legislation.

- Cooperation with the private sector tends to be high, but only around 56 Percent of the examined Member States have established institutionalised forms of cooperation in forms of public-private partnerships

- Legalisation and corresponding obligations for CII-operators vary across sectors. The critical sectors with the strongest regulations across all analysed Member States are the Telecommunications, Finance and Energy sectors

- The majority of countries have conducted a risk assessment on a national level (or are planning to do so). Other countries have decided that risk assessment is the responsibility of sector-specific agencies or of the individual operators.

- Three profiles of CIIP-governance have been identified: A centralised, a decentralised and a co-regulation approach.

Finally, the study makes general recommendations to EU Member States and the EU Commission on how to improve CIIP in the European Union. The recommendations are the following:

Member States

- Recommendation 1: Increase institutionalised cooperation with private stakeholders

- Recommendation 2: Align management structure for CIIP with existing national crisis and emergency management structures

- Recommendation 3: Participate in or [*sic*.] host international exercises

- Recommendation 4: Establish mandatory security incident reporting

- Recommendation 5: Conduct national risk assessment

- Recommendation 6: Utilize best legal framework practices for CIIP across critical sectors

- Recommendation 7: Examine if positive incentives can be provided to operators of CII to invest in security measures

European Commission

- Recommendation 8: Define baseline requirements in order to support the development of CIIP in MS

- Recommendation 9: Develop and conduct a maturity assessment of Member States 'CIIP readiness

- Recommendation 10: Support information sharing and the exchange of knowledge between EU

Member States 'national CSIRTs

- Recommendation 11: Identify European Critical Information Infrastructure

(…)

1.3 CIIP Governance in the European Union Member States (Annex) (January 2016)

Introduction

This analysis is part of a bigger study regarding Stocktaking, Analysis and Recommendation on the Protection of critical information infrastructure (CII), and uncovers the different governance structures for critical information infrastructure protection (CIIP) in 15 EU Member States and 1 EFTA country.

The analysis focuses on CIIP Governance and specifically on the following topics:

- Leading Authorities

- Management Structures

- Roles & Responsibilities

- Relevant Framework (papers and regulations)

- Obligations and requirements for operators of CII (Are operators obligated to implement security measures, e.g. Business Continuity Management?)

(...)

The purpose of this analysis is to better understand the CIIP governance structure in the EU Member States and to analyse the different profiles based on the approaches and commonalities followed by different countries.

(...)

1.4 The cost of incidents affecting CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII) (August 2016)

Executive Summary

Critical Information Infrastructures (CIIs) provide resources upon which several functions of society depend. A potential unavailability of these, would have a debilitating effect on the security, economy and health of society as a whole. Cyber security incidents affecting CIIs are considered nowadays global risks that can have "significant negative impact for several countries or industries within the next 10 years". As more and more businesses/industries benefit from the advantages of information technology, by witnessing a tighter cyber-physical systems integration, developed under concept like Internet of Things, cyber-attacks or incidents affecting those infrastructures are increasing dramatically, resulting in a new chapter in information security; one that can be called Security of Things. While modern economies rely on the newly developed cyber infrastructures, assuring their security has become the main priority of many actors (governments, companies etc.) as this may have implications for the protection the economies and of business.

A prevalent challenge has been to identify the exact magnitude of incidents in terms of cost required for full recovery, and to determine the national or EU-wide economic impact. The purpose of this document is to take a first step in responding to this challenge, through which we have tried to identify if we currently are able to determine the real impact of incidents and if not what can we do in the future to enable that.

Although there is a plethora of studies addressing the economic impact of incidents, each one of them examines the topic from a different perspective, focusing on certain industries, using different metrics, counting only certain types of incidents etc. The lack of a common approach and criteria for performing such an analysis has allowed the development of rarely comparable standalone studies, often relevant only in a certain context. Despite the lack of relevant studies in EU on this topic, the systematic review undertaken allowed us to identify useful findings for future work in the field, and build an early impression on the current EU and worldwide status.

In this respect, the review revealed that cyber-incidents are a real problem, manifested through a particular set of threats affecting similar types of assets, resulting in financial loss. Among the main findings are the following:

- Finance, ICT and Energy sectors, appear to have the highest incident costs.

- The most common attack types for Financial sector and ICTs appear to be DoS/DDoS and malicious insiders, with the latter affecting the Public Administration sector as well. It is very important to highlight that these two types on their own, collectively constitute approximately half the annualized cost of all cybercrime...

- The most expensive attacks are considered to be insider threats, followed by DDoS and web based attacks.

- In terms of country loss the values provided reach up to 1.6% of GDP in some EU countries. Other studies mention figures like 425,000 to 20 million euro per company per year (Germany). Another study provides the average cost per company per year that can vary between 2.3 mil. and 15 mil. euro in 2015. One study also estimates the economic loss for the global economy to be from 330 to 506 billion euro (375 to 575 billion $).

- Data seems to be the most affected asset.

Besides the common findings identified above, each study has produced its own set of findings, mostly relevant in their particular context:

- Cybercrime continues to be on the rise, with the cost varying and depending on the organisational size.

- Countries are likely to tolerate malicious activity as long as it stays at acceptable levels, less than 2% of national income; but measuring the exact impact proves to be difficult.

- Business disruption represents the highest external cost, followed by costs associated with information loss.

- The urgency to prepare and invest in incident response usually occurs only after an event with a significant impact.

- The best data related to cybercrime comes from the financial sector, which is regulated, pays serious attention to cybersecurity, and can easily measure loss being also one of the most targeted industry.

- Companies are in need of qualified personnel, but in some cases they lack completely. Employing under-qualified employees implies a higher risk.

- Governments need to collect and publish data on cybercrime, and help countries and companies to make better choices about risk and policy.

- The most affected CII sectors seem to be financial, ICT and energy.

- A large majority of organisations still have not implemented basic security controls.

- Attackers are streamlining and upgrading their techniques, while companies struggle to fight old tactics.

- In most cases, attackers are able to compromise an organization within minutes, while time to recover takes considerably longer.

- The large majority of vulnerabilities were exploited one year or more after the vulnerability was revealed; patch management is therefore still one of the weakest links.

In terms of conclusions reached among the most notable one is that the measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task. Determining cost values that are as close as possible to reality is a key to determining the real economic impact of incidents on EU's economy. Knowing the real impact can help define proper, coherent and cost effective (beneficial) mitigation policies. As a short note, the NIS directive states that "[...] incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union", without making any use of figures in support of this. We have also noticed the lack of a unified and standardised approach in developing such studies, often driven by business factors rather than actual interest of stakeholders or realistic needs

(...)

1.5 Critical Cloud Computing: A CIIP perspective on cloud computing services (December 2012)

Executive summary

Public and private sector organisations are switching to cloud computing. While some years ago applications would be mainly run on servers on their own premises or dedicated data centres, now applications are outsourced to large cloud service providers and run in a few large data centres. Public data on the uptake of cloud computing shows that in a couple of years around 80% of organisations will be dependent on cloud computing. Large cloud providers will be serving tens of millions of end-users.

From a CIIP perspective this concentration of IT resources is a 'double edged sword': On the one hand, large cloud providers can deploy state of the art security and resilience measures and spread the associated costs across the customers. On the other hand, if an outage or a security breach occurs the consequences could be big, affecting a lot of data, many organizations and a large number of citizens, at once. In fact in the last year there were a number of outages affecting several very large sites with millions of users.

The EU member states have committed to protecting critical ICT systems via the European Commission's CIIP action plan by preventing large cyber-attacks and cyber disruptions of critical ICT systems. In the follow-up the European commission asks for a discussion about a governance strategy for cloud computing services, in the context of CIIP.

In this report we look cloud computing from a CIIP perspective and we look at a number of scenarios and threats relevant from a CIIP perspective, based on a survey of public sources on uptake of cloud computing and large cyber attacks and disruptions of cloud computing services.

From the scenarios and the data about uptake and incidents we draw a number of conclusions.

- Cloud computing is critical: Cloud computing usage is growing and in the near future the vast majority of organizations will rely on some form of cloud computing services. This makes cloud computing services critical in themselves. When cyber attacks and cyber disruptions happen, millions of users are affected. Cloud computing is being adopted also in critical sectors, like finance, energy and transport.

- Cloud computing and natural disasters: A key benefit of cloud computing is resilience in the

face of regional power cuts or local natural disasters. It is difficult to mitigate the impact of fairly common regional disasters like floods, storms, or earthquakes in a set up with only a single datacentre, or a traditional set-up with a legacy onsite IT deployment.

- Cloud computing and overloads or DDoS attacks: Elasticity is a key benefit of cloud computing and this elasticity helps to cope with load and mitigates the risk of overload or DDoS attacks. It is difficult to mitigate the impact of peak usage or a DDoS attack with limited computing resources.

- Cyber attacks: Cyber attacks which exploit software flaws can cause very large data breaches, affecting millions of users directly. The impact of cyber attacks is multiplied by the concentration of resources which is a result of the uptake in cloud computing.

- Infrastructure and platform as a Service the most critical: The most critical services are large IaaS and PaaS services which deliver services to other IT vendors who service in turn millions of users and organisations.

- Administrative and legal disputes: Cloud computing is not immune to administrative or legal issues. If there is a legal dispute involving the provider or one of its customers, than this could have an impact on the data of all the other co-customers (or co-tenants).

The CIIP action plan calls for a discussion about governance strategies for cloud computing and also in speeches about the EU Cyber Security Strategy the issue of cyber security governance is addressed. Below we make a number of recommendations related to the issue of national governance of critical cloud computing services.

Governance, from a national perspective, can be split into three key processes: 1) Risk assessment, 2) ensuring that appropriate security measures are taken, and 3) collecting incident reports.

Risk assessment: Risk assessment is the basis for security governance.

- Assets in scope: It is important to take a pragmatic approach and address the most critical cloud computing services first. It is easy to say that ‘all cloud computing services are critical ’but it is infeasible to address everything at once. As mentioned, since outages at IaaS or PaaS providers can have an impact across a range of organizations, this means that they should be treated with priority.

- Assessing dependencies on cloud computing: Most countries, when making national risk assessments, from a critical infrastructure perspective, take into account power supply and electronic communications networks. Public sources on uptake cloud computing suggest that it is necessary to take into account also large cloud computing services and large datacentres.

- Transparency about logical and physical dependencies: A risk assessment requires a clear view of the dependencies. It should be clear which critical operators and critical services depend on which cloud computing services. The special nature of cloud computing creates resilience but it can also increase interdependencies and cause cascading failures. Outages at an underlying IaaS or PaaS provider can affect a range of (otherwise unrelated) services across society. It is important to map all the main logical and physical dependencies.

Security measures: Taking appropriate security measures is the focus of security governance.

- Foster exchange of best practices to achieve a security baseline: It goes without saying that it is important that cloud providers take appropriate security measures. These measures should be based on best-practices. It is important for government authorities to support and foster the exchange of such best practices. Security is constantly changing and security measures must be improved continuously. Government authorities should encourage an open culture of exchange and discussion about security measures. Security is about continuous improvement and government authorities should avoid a situation where a specific set of best practices is cast in stone (by regulation or self-regulation).

- Logical redundancy: Cloud computing services are often set-up with several redundant datacentres to withstand outages of single datacentres (due to power cuts or natural disasters, for example). Many cyber attacks, however, capitalise and exploit software flaws, which are persist across the datacentres. It is important to prevent and mitigate the impact of cyber attacks by creating also logical redundancy – that is, to use different layers of defence and to use separate systems with a different logical structure, to cross-check transactions and to detect attacks.

- Standardisation: From a CIIP perspective standardization in cloud computing is very important, because it allows customers to mitigate issues related to a specific provider or a specific platform. Standardization, especially for IaaS and PaaS services, would allow customers to move workload to other providers in case one provider has suffers a large outages caused by system failures or even administrative or legal disputes.

- Monitoring, audits, tests, and exercises: There is a lot of information security literature about the importance of auditing and testing systems. Cloud computing providers should schedule frequent audits and tests, by internal testers and auditors, and, when relevant, by external testers and auditors. In discussions about governance, often the need for certification, by independent external auditors is stressed. But it is hard for an external auditor to assess the security of a complex and continuously changing system, by performing an audit once per year. Cloud computing providers and government authorities should have a continuous program of monitoring, audits, tests and exercises in place. Yearly audits by external parties are only a small part of such a program.

Incident reporting: Incident reporting provides a cross-check on the security measures, it provides the input for an improved risk assessment, and it provides strategic feedback about the overall governance process.

- Mandatory reporting: Without incident reports it is very difficult to understand the impact of security incidents on cloud computing providers. This complicates risk assessment, both for cloud computing service providers, as well as, at a national level, for government authorities like agencies responsible for (civil) contingency planning. Lack of data about incidents makes it very difficult to prioritize security measures, and in this way security governance becomes inefficient or even ineffective. Government authorities and cloud providers should agree on the thresholds for reporting and the type of services that should be in scope.

- Legal consequences: Secondly, it is important to consider that certain cyber attacks are stealthy and their traces may be difficult to spot even for system administrators who know the cloud computing systems inside out. There is always a risk that security incidents are not reported to higher management or to authorities for fear of reprisal or legal consequences. Member states should consider giving incentives to providers who report security breaches which would otherwise go unnoticed.

(…)

1.6 Protecting Industrial Control Systems: Recommendations for Europe and Member States (2011)

Executive summary

Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes. These systems are responsible for monitoring and controlling a variety of processes and operations such as gas and electricity distribution, water treatment, oil refining or railway transportation. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems. In the last few years, ICS have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet. Today, ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the-shelf software. All this has led to cost reductions, ease of use and enabled the remote control and monitoring from various locations. However, an important drawback derived from the connection to intranets and open communication networks, is the increased vulnerability to computer network-based attacks.

Industrial control systems constitute a strategic asset against the rising potential for catastrophic terrorist attacks affecting critical infrastructures. In the last decade, these systems have been facing a notable number of incidents, including the manifestation of Stuxnet which raised a lot of concerns and discussions among all the actors involved in the field.

In April 2007, the Council adopted the conclusions of a European programme for critical infrastructure protection (EPCIP). This was the result of a series of actions driven by the European Commission, the Council and the Justice and Home Affairs Council which started in June 2004. The key element of EPCIP is the Directive on the identification and designation of European Critical Infrastructures. In parallel, the information security issues for vital infrastructures in Europe are addressed by The Digital Agenda for Europe (DAE) and the CIIP action plan.

Recognising the importance of the problem, ENISA launched a series of activities, which aim at bringing together the relevant stakeholders and engaging them into an open discussion on ICS protection. The principal goal of the open dialogue is to identify the main concerns regarding the security of ICS as well as to recognize and support national, pan European and international initiatives on ICS security. The involved stakeholders include ICS security tools and services providers, ICS software/hardware manufactures and integrators, infrastructure operators, public bodies, standardisation bodies, academia and R&D.

Furthermore, in order to help the stakeholders get a deeper insight on the issue, ENISA decided to further explore this problem by delivering a research and survey-based study on this topic. The objective of the study is to obtain the current perspective of ICS protection primarily in Europe, but also in the international context. This view includes threats, risks and challenges in the area of ICS protection as well as national, pan European and international initiatives on ICS security.

This final report proposes 7 recommendations to the public and private sector involved in the area of Industrial Control Systems. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, developing new measures and good practices, and reducing barriers to information sharing. This guidance is based on the results of a thorough analysis of the opinions of the experts who participated in the Study. Furthermore, important information coming from an in depth desktop investigation is also taken into consideration. All this data has been analysed and has led to the derivation of almost 100 Key Findings.

What follows is a brief summary of all the recommendations.

Recommendation 1: Creation of Pan-European and National ICS Security Strategies. The European Union should create a pan-European Strategy for European ICS Security activities and each Member State should develop a National Strategy for ICS Security. The strategies must be coherent with the European Union Council Directive 2008/114/EC for Critical Infrastructures, and leveragethe existing initiatives addressing the problem of ICS Security (e.g. EuroSCSiE) as well as the national and Pan-European Public Private Partnerships (e.g. EP3Rs). The strategies have to serve as references for all state-members stakeholders, act as facilitators for sharing initiatives and foster research and education.

Recommendation 2: Creation of a Good Practices Guide for ICS security. The European Union should assume leadership and develop a consensus-reached document or set of documents regarding security good practices, integrating both physical and logical security aspects, to serve as reference for every type of stakeholder. This document should help all stakeholders ensure that best security practices are applied in the industry.

Recommendation 3: Creation of ICS security plan templates. The different National ICS Security Strategies should consider within their tasks the creation of ICS security plan templates, both for operator and infrastructures, which security experts could adapt to their particular situation. These plans should include operational and physical security, technical issues, training and awareness, security governance with roles and responsibilities, business impact measures and crisis management. These templates should severely decrease the cost of developing security plans and accelerate the adoption of comprehensive security measures within the industry.

Recommendation 4: Foster awareness and training. As part of national ICS-Security strategies, the Member States should foster dissemination and awareness activities through high quality events involving all kinds of stakeholders and with special attention to top management commitment. Training and awareness programmes and events should be created for all types of end users.

Recommendation 5: Creation of a common test bed, or alternatively, an ICS security certification framework. The Common ICS-Strategy should lead to the creation of a common test bed(s) at European level, as a Public-Private Partnership in which tests could be performed in order to guarantee that different systems interaction do not cause security failures. A common test bed will help all stakeholders to detect potential problems in a controlled environment, ensuring integrity and increasing the trustfulness in certified solutions.

Alternatively a security framework model adapted for ICS could be defined, based on existing efforts such as Common Criteria or FIPS. Member State existing certifying organisms would be responsible for the certification process based on this security framework.

Recommendation 6: Creation of national ICS-computer emergency response capabilities. Following the national ICS Security Strategies, national ICS-computer emergency response capabilities should be established, in cooperation with an adequate number of public and private CERTs. The ICS-computer emergency response capabilities should help all stakeholders to have a reference in order to share vulnerability information, disclosure it, coordinate actions and help in effectively dealing with risk management in ICS infrastructures. In order to address the challenges which span across the borders, member states should cooperate on the Pan-European level (e.g. with the aid of an ICS-Security information sharing platform such as EuroSCSiE).

Recommendation 7: Foster research in ICS security leveraging existing Research Programmes. The National and Common ICS Security Strategies should foster research to address current and future ICS threats and security challenges such as ICS-ICT integration, legacy/insecure equipment, targeted attacks or Smart Grid issues. This should be done by leveraging existing European or National research programmes, such as the European Framework Programme.

(…)

1.7 Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors (2015)

Executive Summary

ICS (Industrial Control Systems) is a general term describing industrial automation systems responsible for data acquisition, visualization and control of industrial processes, often found in various industrial sectors and Critical Infrastructures. They play a critical role not only in maintaining the continuity of industrial processes but also to ensure functional and technical safety, preventing large industrial accidents and environmental disasters.

The criticality of control systems in vital sectors, and high impact in case of disruption, makes them a major target for malicious activities. Based on the ICS-CERT Monitor (part of U.S. Department of Homeland Security)1, between 2009 and 2014 the number of reported cyber security incidents in the ICS-SCADA area increased more than 27 times. At the same time more than half of the incidents (59% in 2013) were aimed at the energy and critical manufacturing sectors and around 55% involved advanced persistent threats (APT). Still many ICS-SCADA cyber security incidents stay undetected or unreported.

(...)

This study reveals the current maturity level of ICS- SCADA cyber security in Europe and identifies good practices used by European Member States to improve this area.

The first and second part of this study introduces us to the ICS-SCADA cyber security topic, explains the role of ICS-SCADA in critical sectors and summarizes the methodology of this study.

During the desk research, current activities of different Member States in the area of ICS-SCADA cyber security were identified, including related activities, legislation status, existing cyber security strategies and the responsibility matrix of entities dedicated to improve the level of ICS-SCADA cyber security in each country.

Following the research, the ICS-SCADA Cyber Security Maturity Model was used while performing a series of interviews with designated officials from eight Member States. As a result, four Maturity Profiles were identified and described in the third part of this study:

- Leading - Member States with strong legislation and supporting mechanisms dedicated to ICS SCADA cyber security improvement

- Proactive Supporters - Member States focused on strong Critical Infrastructure operators support and driving the ICS SCADA cyber security improvement

- Reactive Supporters - Member States focused on lessons learned and reactive means of improving ICS SCADA cyber security

- Early Developers - Member States in the process of developing of legislation and supporting system to protect ICS SCADA in Critical Infrastructure

The analysis of maturity level reveals areas for improvement which are concluded in the fifth and last part of this study. As a result, a set of high level and context specific future recommendations to policy and decision makers are issued that include, among others:

Recommendation 1: Align ICS-SCADA efforts with national cyber security strategies and CIIP effort. Currently ICS-SCADA cyber security is not aligned with National Cyber Security Strategies (NCSS) and Critical Information Infrastructure Protection (CIIP) efforts. National Cyber Security Strategies create a baseline for defining cyber space, cyber security objectives and areas of actions. As the ICS-SCADA area is an integral part of the National and EU cyberspace and Critical Infrastructures, it should be aligned with the NCSS as well as CIIP efforts.

Recommendation 2: Develop good practices specific to ICS-SCADA cyber security. Many Member States do not use industry good practices as a reference to set-up an ICS-SCADA cyber security baseline for Critical Sectors. Multiple guidelines, ICS-SCADA security standards and good practices are already developed in the ICS community as well as by individual Member States. It is recommended to leverage from this to develop a minimum security baseline and good practices for ICS-SCADA in Critical Sectors in EU.

Recommendation 3: Standardize information sharing among critical sectors and Member States. Information sharing on ICS-SCADA cyber security incidents and good practices are not communicated in a standardized and frequent manner. A special emphasis should be given on standardizing information sharing of good practices and known threats across critical sectors. A single platform and process (e.g. ICS CERT) to report cyber security incidents and good practices should be in place. Trust between Critical Information Infrastructure (CII) operators and the platform should be built to ensure effective communication from as well as towards the operators.

Recommendation 4: Build ICS-SCADA cyber security awareness. Special emphasis should be given on building awareness of ICS-SCADA cyber security aspects not only across CII operators, but also among decision and policy makers. Nowadays the awareness is built mainly on serious security breaches and incidents. This underlines the more reactive approach, which should be moved towards a continuous awareness growth. As a consequence the ICS-SCADA cyber security threats should be well understood and considered separate from Information Technology (IT) security. This could be achieved by organizing ICS-SCADA cyber security related events involving sector specific platforms to share current challenges and good practices. Knowledge sharing and awareness building should result directly from the ICS-SCADA cyber security strategies.

Recommendation 5: Foster expertise with ICS-SCADA cyber security trainings [*sic*.] and educational programmes. Current ICS-SCADA cyber security threats multiply at a very rapid pace. Also several more robust and technology advanced attacks (e.g. Advanced Persistent Threat - APT) are aimed at ICS systems. Moreover a lot of ICS-SCADA cyber security aspects are considered the same as in IT. This basic misunderstanding very often leads to security flaws in ICS-SCADA environments. A deep understanding of the process as well as the technology is needed in order to perceive the real risk and focus area for improving ICS-SCADA cyber security. This is why it is so important to develop future experts and leaders in the area of ICS-SCADA cyber security. This could be done by setting up and supporting new study programs for ICS-SCADA security as well as organizing and promoting related trainings among public bodies.

Recommendation 6: Promote and support ICS-SCADA cyber security research and test beds. It is necessary to involve ICS-SCADA experts and system vendors in the process of addressing current and future cyber security related threats. Support in research programmes and creation of common test-beds can foster ICS-SCADA cyber security innovation and improve security-by-design concept.

The recommendations shall assist, both the European Commission and the Member States, in the process of building resilient ICS-SCADA environment in Europe.

(…)

1.8 Certification of Cyber Security skills of ICS/SCADA professionals: Good practices and recommendations for developing harmonised certification schemes (December 2014)

Executive summary

The industrial world is constantly evolving, including new technologies adapting to market requirements. One of the most transcendental adaptations the industrial world is currently experiencing is the convergence between Operations Technology (OT), the operations needed to carry out the industrial processes, and Information Technology (IT), the use of computers to

manage data needed by the organisation's enterprise processes. This convergence has many advantages (optimisation of operations, better use of resources, cost savings, etc.), but it also raises additional issues, such as the need for cyber security of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

This convergence, which affects hundreds of thousands of systems worldwide, implies that professionals with knowledge of cyber security for ICS/SCADA will be needed. However, currently, there are very few professionals with the proven skills available to do this work.

This document explores how current initiatives on certification of professional skills are related to the topic of ICS/SCADA cyber security. It also identifies the challenges and proposes a series of recommendations towards the development of certification schemes for ICS/SCADA cyber security professionals.

Challenges identified in relation to operational issues of certifications included the following:

- The need to handle the confluence of contents, objectives and needs of two very different topics such as cyber security and industrial automation within a number of different industrial sectors (energy, oil & gas, automated manufacturing, water treatment, chemical, pharmaceutical, etc.)

- The complexity of including topics and content relevant to different roles and profiles. In the field of cyber security for ICS/SCADA systems there are implications ranging from the lower operative levels to the top management.

- The challenge to include an important practical component, in future certification contents, able to take into account the nature of the operations performed over industrial control systems. This can be a complicated issue since the operations where ICS are involved, usually need to be executed continuously making it difficult to put them in practice on production systems.

Challenges related to the societal aspects include the following:

- Avoiding commercial interests that could impair the credibility of certifications.

- Obtaining stakeholders 'support to underscore the relevance, credibility and strength of future certifications.

- Ensuring that the future certifications will improve compared with existing ones in regards the level of knowledge related to cyber security for ICS/SCADA.

- Exploring the professional roles and specific knowledge needed by cyber security professionals for ICS/SCADA.

Pursuant to interviews with experts worldwide and the analysis of the results of an online survey, this report proposes a series of recommendations for the development of cyber security certifications for ICS/SCADA professionals.

This report concludes that the development of an overarching certification scheme is of paramount importance to allow European professionals to achieve the degree of measured knowledge needed to deal with the cyber security issues in ICS/SCADA systems. This would create a suitable workforce for European industrial organisations to face the cyber security challenges related to these systems. Certification should be multi-level to allow reaching a wide range of professionals from different fields of practice; it should include not only operational but managerial topics and it should contain practical aspects, to guarantee that the knowledge of certified professionals is not only theoretical and can be directly applied to industrial operations...

(…)

1.9 Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (November 2017)

Executive Summary

The Internet of Things (IoT) is a growing paradigm with technical, social, and economic significance. For ENISA, IoT is an emerging concept comprising a wide ecosystem of interconnected services and devices, such as sensors, consumer products and everyday smart home objects, cars, and industrial and health components. These technologies collect, exchange and process data in order to dynamically adapt to a specific context, transforming the business world and the way we live as a whole. IoT is tightly bound to cyber-physical systems and, in this respect, safety implications are pertinent.

Nevertheless, IoT poses very important safety and security challenges that need to be addressed for IoT to reach its full potential. Many security considerations regarding IoT are not necessarily new; they are inherited from the use of networking technologies. However, the characteristics of some IoT implementations present new security challenges, threats and risks that are manifold and evolve rapidly. The protection of IoT deployments depends on the protection of all systems involved (the devices themselves, cloud backend and services, applications, maintenance and diagnostic tools, etc.).

Addressing these challenges and ensuring security in IoT products and services is a fundamental priority. One of the main concerns is the impact that the different threats may have since attacks on IoT deployments could dramatically jeopardise people's security, privacy and safety, while additionally IoT in itself can be used as an attack vector against other critical infrastructures. Also, since IoT can drastically change the ways personal data is collected, analysed, used, and protected, privacy concerns have been raised. These need to be addressed to ensure user trust and confidence in the Internet, connected devices, and related services.

However, beyond technical security measures, the adoption of IoT has raised many new legal, policy and regulatory challenges, broad and complex in scope, that remain unanswered, amplifying at the same time some existing issues. The rapid rate of change in IoT technology has outpaced the ability of the associated policy, legal, and regulatory structures to adapt, leaving no clear security framework to follow. This has led most companies and manufacturers to take their own approach when designing IoT devices, causing interoperability issues between devices from different manufacturers, and between IoT devices and legacy systems.

For these reasons, ENISA is defining a set of Baseline Security Recommendations for IoT. The aim of this work as reported here is to provide insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems.

As a result of this work, after taking into consideration all the background research carried out, the views expressed by the experts interviewed, and the good practices and security measures identified, a series of recommendations has been developed, namely:

- Promote harmonization of IoT security initiatives and regulations: Intended for IoT industry, providers, manufacturers, associations

- Raise awareness for the need for IoT cybersecurity: Intended for IoT industry, providers, manufacturers, associations, academia, consumer groups, regulators

- Define secure software/hardware development lifecycle guidelines for IoT: Intended for IoT developers, platform operators, industry, manufacturers

- Achieve consensus for interoperability across the IoT ecosystem: Intended for IoT industry, providers, manufacturers, associations, regulators

- Foster economic and administrative incentives for IoT security: Intended for IoT industry, associations, academia, consumer groups, regulators

- Establishment of secure IoT product/service lifecycle management: Intended for IoT developers, platform operators, industry, manufacturers

- Clarify liability among IoT stakeholders Intended for IoT industry, regulators

(…)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

(…)

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross- border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

(5) The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas.

(6) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers. However, operators of essential services and digital service providers are not precluded from implementing security measures that are stricter than those provided for under this Directive.

(7) To cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers. However, the obligations on operators of essential services and digital service providers should not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council, which are subject to the specific security and integrity requirements laid down in that Directive, nor should they apply to trust service providers within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council, which are subject to the security requirements laid down in that Regulation.

(8) This Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of the essential interests of its security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences. In accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU), no Member State is to be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security. In this context, Council Decision 2013/488/EU and non-disclosure agreements, or informal non-disclosure agreements such as the Traffic Light Protocol, are of relevance.

(9) Certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of network and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive. Member States should then apply the provisions of such sector-specific Union legal acts, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by this Directive. In this context, Member States should provide information to the Commission on the application of such *lex specialis* provisions. In determining whether the requirements on the security of network and information systems and the notification of incidents contained in sector-specific Union legal acts are equivalent to those contained in this Directive, regard should only be had to the provisions of relevant Union legal acts and their application in the Member States.

(10) In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as *lex specialis*, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive.

(11) When identifying operators in the water transport sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach.

(12) Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonised at Union level, through the use of primary and secondary Union law and standards developed together with the European supervisory authorities. Within the banking union, the application and the supervision of those requirements are ensured by the single

supervisory mechanism. For Member States that are not part of the banking union, this is ensured by the relevant banking regulators of Member States. In other areas of financial sector regulation, the European System of Financial Supervision also ensures a high degree of commonality and convergence in supervisory practices. The European Securities Markets Authority also plays a direct supervision role for certain entities, namely credit-rating agencies and trade repositories.

(13) Operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructures. It covers all operations including the security, integrity and resilience of network and information systems. The requirements in respect of those systems, which often exceed the requirements provided for under this Directive, are set out in a number of Union legal acts, including: rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and rules on prudential requirements for credit institutions and investment firms, which include requirements concerning operational risk; rules on markets in financial instruments, which include requirements concerning risk assessment for investment firms and for regulated markets; rules on OTC derivatives, central counterparties and trade repositories, which include requirements concerning operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the Union and on central securities depositories, which include requirements concerning operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider those rules and requirements in their application of *lex specialis*.

(14) As noted by the European Central Bank in its opinion of 25 July 2014, this Directive does not affect the regime under Union law for the Eurosystem's oversight of payment and settlement systems. It would be appropriate for the authorities responsible for such oversight to exchange experiences on matters concerning security of network and information systems with the competent authorities under this Directive. The same consideration applies to non-euro area members of the European System of Central Banks exercising such oversight of payment and settlement systems on the basis of national laws and regulations.

(15) An online marketplace allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services through which a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product. Computing services provided by the online marketplace may include processing of transactions, aggregations of data or profiling of users. Application stores, which operate as online stores enabling the digital distribution of applications or software programmes from third parties, are to be understood as being a type of online marketplace.

(16) An online search engine allows the user to perform searches of, in principle, all websites on the basis of a query on any subject. It may alternatively be focused on websites in a particular language. The definition of an online search engine provided in this Directive should not cover search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine. Neither should it cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product.

(17) Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this Directive, the term ‘cloud computing services ’covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term ‘scalable ’refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources,

in order to handle fluctuations in demand. The term ‘elastic pool ’is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term ‘shareable ’is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

(18) The function of an internet exchange point (IXP) is to interconnect networks. An IXP does not provide network access or act as a transit provider or carrier. Nor does an IXP provide other services unrelated to interconnection, although this does not preclude an IXP operator from providing unrelated services. An IXP exists to interconnect networks that are technically and organisationally separate. The term ‘autonomous system ’is used to describe a technically stand-alone network.

(19) Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services. In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all Member States. To that end, this Directive provides for the assessment of the entities active in specific sectors and subsectors, the establishment of a list of essential services, the consideration of a common list of cross-sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in the case of entities providing services in more than one Member State, and the support of the Cooperation Group in the identification process. In order to ensure that possible changes in the market are accurately reflected, the list of identified operators should be reviewed regularly by Member States and updated when necessary. Finally, Member States should submit to the Commission the information necessary to assess the extent to which this common methodology has allowed a consistent application of the definition by Member States.

(20) In the process of identification of operators of essential services, Member States should assess, at least for each subsector referred to in this Directive, which services have to be considered as essential for the maintenance of critical societal and economic activities, and whether the entities listed in the sectors and subsectors referred to in this Directive and providing those services meet the criteria for the identification of operators. When assessing whether an entity provides a service which is essential for the maintenance of critical societal or economic activities, it is sufficient to examine whether that entity provides a service that is included in the list of essential services. Furthermore, it should be demonstrated that provision of the essential service is dependent on network and information systems. Finally, when assessing whether an incident would have a significant disruptive effect on the provision of the service, Member States should take into account a number of cross-sectoral factors, as well as, where appropriate, sector-specific factors.

(21) For the purposes of identifying operators of essential services, establishment in a Member State implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary possessing legal personality, is not the determining factor in this respect.

(22) It is possible that entities operating in the sectors and subsectors referred to in this Directive provide both essential and non-essential services. For example, in the air transport sector, airports provide services which might be considered by a Member State to be essential, such as the management of the runways, but also a number of services which might be considered as non-essential, such as the provision of shopping areas. Operators of essential services should be subject to the specific security requirements only with respect to those services which are deemed to be essential. For the purpose of identifying operators, Member States should therefore establish a list of the services which are considered as essential.

(23) The list of services should contain all services provided in the territory of a given Member State that fulfil the requirements under this Directive. Member States should be able to supplement the existing list by including new services. The list of services should serve as a reference point for Member States, allowing for identification of operators of essential services. Its purpose is to identify the types of essential services in any given sector referred to in this Directive, thus distinguishing them from non-essential activities for which an entity active in any given sector might be responsible. The list of services established by each Member State would serve as further input in the assessment of the regulatory practice of each Member State with a view to ensuring the overall level of consistency of the identification process amongst Member States.

(24) For the purposes of the identification process, where an entity provides an essential service in two or more Member States, those Member States should engage in bilateral or multilateral discussions with each other. This consultation process is intended to help them to assess the critical nature of the operator in terms of cross-border impact, thereby allowing each Member State involved to present its views regarding the risks associated with the services provided. The Member States concerned should take into account each other's views in this process, and should be able to request the assistance of the Cooperation Group in this regard.

(25) As a result of the identification process, Member States should adopt national measures to determine which entities are subject to obligations regarding the security of network and information systems. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria, such as the output of the operator or the number of users, which make it possible to determine which entities are subject to obligations regarding the security of network and information systems. The national measures, whether already existing or adopted in the context of this Directive, should include all legal measures, administrative measures and policies allowing for the identification of operators of essential services under this Directive.

(26) In order to give an indication of the importance, in relation to the sector concerned, of the identified operators of essential services, Member States should take into account the number and the size of those operators, for example in terms of market share or of the quantity produced or carried, without being obliged to divulge information which would reveal which operators have been identified.

(27) In order to determine whether an incident would have a significant disruptive effect on the provision of an essential service, Member States should take into account a number of different factors, such as the number of users relying on that service for private or professional purposes. The use of that service can be direct, indirect or by intermediation. When assessing the impact that an incident could have, in terms of its degree and duration, on economic and societal activities or public safety, Member States should also assess the time likely to elapse before the discontinuity would start to have a negative impact.

(28) In addition to the cross-sectoral factors, sector-specific factors should also be considered in order to determine whether an incident would have a significant disruptive effect on the provision of an essential service. With regard to energy suppliers, such factors could include the volume or proportion of national power generated; for oil suppliers, the volume per day; for air transport, including airports and air carriers, rail transport and maritime ports, the proportion of national traffic volume and the number of passengers or cargo operations per year; for banking or financial market infrastructures, their systemic importance based on total assets or the ratio of those total assets to GDP; for the health sector, the number of patients under the provider's care per year; for water production, processing and supply, the volume and number and types of users supplied, including, for example, hospitals, public service organisations, or individuals, and the existence of alternative sources of water to cover the same geographical area.

(29) To achieve and maintain a high level of security of network and information systems, each Member State should have a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented.

(30) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of operators of essential services and digital service providers under this Directive.

(31) In order to facilitate cross-border cooperation and communication and to enable this Directive to be implemented effectively, it is necessary for each Member State, without prejudice to sectoral regulatory arrangements, to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level. Competent authorities and single points of contact should have the adequate technical, financial and human resources to ensure that they can carry out the tasks assigned to them in an effective and efficient manner and thus achieve the objectives of this Directive. As this Directive aims to improve the functioning of the internal market by creating trust and confidence, Member State bodies need to be able to cooperate effectively with economic actors and to be structured accordingly.

(32) Competent authorities or the computer security incident response teams ('CSIRTs') should receive notifications of incidents. The single points of contact should not receive directly any notifications of incidents unless they also act as a competent authority or a CSIRT. A competent authority or a CSIRT should however be able to task the single point of contact with forwarding incident notifications to the single points of contact of other affected Member States.

(33) To ensure the effective provision of information to the Member States and to the Commission, a summary report should be submitted by the single point of contact to the Cooperation Group, and should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers, as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group. The summary report should include information on the number of notifications received, as well as an indication of the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.

(34) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. In order for all types of operators of essential services and digital service providers to benefit from such capabilities and cooperation, Member States should ensure that all types are covered by a designated CSIRT. Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.

(35) As most network and information systems are privately operated, cooperation between the public and private sectors is essential. Operators of essential services and digital service providers should be encouraged to pursue their own informal cooperation mechanisms to ensure the security of network and information systems. The Cooperation Group should be able to invite relevant stakeholders to the discussions where appropriate. To encourage effectively the sharing of information and of best practice, it is essential to ensure that operators of essential services and digital service providers who participate in such exchanges are not disadvantaged as a result of their cooperation.

(36) ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA. To build capacity and knowledge among Member States, the Cooperation Group should also serve as an instrument for the exchange of best practice, discussion of capabilities and preparedness of the Member States and, on a voluntary basis, to assist its members in evaluating national strategies on the security of network and information systems, building capacity and evaluating exercises relating to the security of network and information systems.

(37) Where appropriate, Member States should be able to use or adapt existing organisational structures or strategies when applying this Directive.

(38) The respective tasks of the Cooperation Group and of ENISA are interdependent and complementary. In general, ENISA should assist the Cooperation Group in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council, namely to assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information system security under existing and future legal acts of the Union. In particular, ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training. ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident.

(39) In order to promote advanced security of network and information systems, the Cooperation Group should, where appropriate, cooperate with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practice, and to provide advice on security aspects of network and information systems that might have an impact on their work, while respecting existing arrangements for the exchange of restricted information. In cooperating with law enforcement authorities regarding the security aspects of network and information systems that might have an impact on their work, the Cooperation Group should respect existing channels of information and established networks.

(40) Information about incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized enterprises. In some cases, such information is already provided via websites at the national level, in the language of a specific country and focusing mainly on incidents and occurrences with a national dimension. Given that businesses increasingly operate across borders and citizens use online services, information on incidents should be provided in an aggregated form at Union level. The secretariat of the CSIRTs network is encouraged to maintain a website or to host a dedicated page on an existing website, where general information on major incidents that have occurred across the Union is made available to the general public, with a specific focus on the interests and needs of businesses. CSIRTs participating in the CSIRTs network are encouraged to provide on a voluntary basis the information to be published on that website, without including confidential or sensitive information.

(41) Where information is considered to be confidential in accordance with Union and national rules on business confidentiality, such confidentiality should be ensured when carrying out the activities and fulfilling the objectives set by this Directive.

(42) Exercises which simulate real-time incident scenarios are essential for testing Member States' preparedness and cooperation regarding the security of network and information systems. The CyberEurope cycle of exercises coordinated by ENISA with the participation of the Member States is a useful tool for testing and drawing up recommendations on how incident-handling at Union level should improve over time. Considering that the Member States are not currently

under any obligation to either plan or participate in exercises, the creation of the CSIRTs network under this Directive should enable Member States to participate in exercises on the basis of accurate planning and strategic choices. The Cooperation Group set up under this Directive should discuss the strategic decisions regarding exercises, in particular but not exclusively as regards the regularity of the exercises and the design of the scenarios. ENISA should, in accordance with its mandate, support the organisation and running of Union-wide exercises by providing its expertise and advice to the Cooperation Group and the CSIRTs network.

(43) Given the global nature of security problems affecting network and information systems, there is a need for closer international cooperation to improve security standards and information exchange, and to promote a common global approach to security issues.

(44) Responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services and digital service providers. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a trustworthy level playing field is also essential to the effective functioning of the Cooperation Group and the CSIRTs network, to ensure effective cooperation from all Member States.

(45) This Directive applies only to those public administrations which are identified as operators of essential services. Therefore, it is the responsibility of Member States to ensure the security of network and information systems of public administrations not falling within the scope of this Directive.

(46) Risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems comprises the security of stored, transmitted and processed data.

(47) Competent authorities should retain the ability to adopt national guidelines concerning the circumstances in which operators of essential services are required to notify incidents.

(48) Many businesses in the Union rely on digital service providers for the provision of their services. As some digital services could be an important resource for their users, including operators of essential services, and as such users might not always have alternatives available, this Directive should also apply to providers of such services. The security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross- border trade across the Union. Those digital service providers that are subject to this Directive are those that are considered to offer digital services on which many businesses in the Union increasingly rely.

(49) Digital service providers should ensure a level of security commensurate with the degree of risk posed to the security of the digital services they provide, given the importance of their services to the operations of other businesses within the Union. In practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers. Therefore, the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Because of their cross-border nature, digital service providers should be subject to a more harmonised approach at Union level. Implementing acts should facilitate the specification and implementation of such measures.

(50) While hardware manufacturers and software developers are not operators of essential services, nor are they digital service providers, their products enhance the security of network and information systems. Therefore, they play an important role in enabling operators of essential services and digital service providers to secure their network and information systems. Such hardware and software products are already subject to existing rules on product liability.

(51) Technical and organisational measures imposed on operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner.

(52) Operators of essential services and digital service providers should ensure the security of the network and information systems which they use. These are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The security and notification requirements should apply to the relevant operators of essential services and digital service providers regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

(53) To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises.

(54) Where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they might wish to require from the providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They should be able to do so by means of contractual obligations.

(55) The definitions of online marketplaces, online search engines and cloud computing services in this Directive are for the specific purpose of this Directive, and without prejudice to any other instruments.

(56) This Directive should not preclude Member States from adopting national measures requiring public-sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public-sector body concerned and not to the cloud computing service provider.

(57) Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope. In addition, this Directive and the implementing acts adopted under it should ensure a high level of harmonisation for digital service providers with respect to security and notification requirements. This should enable digital service providers to be treated in a uniform way across the Union, in a manner proportionate to their nature and the degree of risk which they might face.

(58) This Directive should not preclude Member States from imposing security and notification requirements on entities that are not digital service providers within the scope of this Directive, without prejudice to Member States' obligations under Union law.

(59) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational

and commercial damage for the operators of essential services and digital service providers reporting incidents. In the implementation of the notification obligations, competent authorities and the CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

(60) Digital service providers should be subject to light-touch and reactive ex post supervisory activities justified by the nature of their services and operations. The competent authority concerned should therefore only take action when provided with evidence, for example by the digital service provider itself, by another competent authority, including a competent authority of another Member State, or by a user of the service, that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident. The competent authority should therefore have no general obligation to supervise digital service providers.

(61) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information in order to assess the level of security of network and information systems.

(62) Incidents may be the result of criminal activities the prevention, investigation and prosecution of which is supported by coordination and cooperation between operators of essential services, digital service providers, competent authorities and law enforcement authorities. Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage operators of essential services and digital service providers to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA.

(63) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents.

(64) Jurisdiction in respect of digital service providers should be attributed to the Member State in which the digital service provider concerned has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office in the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This criterion should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment.

(65) Where a digital service provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such a digital service provider is offering services within the Union, it should be ascertained whether it is apparent that the digital service provider is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the digital service provider's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the digital service provider is established, is insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the digital service provider is planning to offer services within the Union. The representative should act on behalf of the digital service provider and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a

written mandate of the digital service provider to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

(66) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level. ENISA should assist Member States through advice and guidelines. To this end, it might be helpful to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council.

(67) Entities falling outside the scope of this Directive may experience incidents having a significant impact on the services they provide. Where those entities consider that it is in the public interest to notify the occurrence of such incidents, they should be able to do so on a voluntary basis. Such notifications should be processed by the competent authority or the CSIRT where such processing does not constitute a disproportionate or undue burden on the Member States concerned.

(68) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to lay down the procedural arrangements necessary for the functioning of the Cooperation Group and the security and notification requirements applicable to digital service providers. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (2). When adopting implementing acts related to the procedural arrangements necessary for the functioning of the Cooperation Group, the Commission should take the utmost account of the opinion of ENISA.

(69) When adopting implementing acts on the security requirements for digital service providers, the Commission should take the utmost account of the opinion of ENISA and should consult interested stakeholders. Moreover, the Commission is encouraged to take into account the following examples: as regards security of systems and facilities: physical and environmental security, security of supplies, access control to network and information systems and integrity of network and information systems; as regards incident handling: incident-handling procedures, incident detection capability, incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; and as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and information systems testing, security assessments and compliance monitoring.

(70) In the implementation of this Directive, the Commission should liaise as appropriate with relevant sectoral committees and relevant bodies set up at Union level in the fields covered by this Directive.

(71) The Commission should periodically review this Directive, in consultation with interested stakeholders, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

(72) The sharing of information on risks and incidents within the Cooperation Group and the CSIRTs network and the compliance with the requirements to notify incidents to the national competent authorities or the CSIRTs might require processing of personal data. Such processing should comply with Directive 95/46/EC of the European Parliament and the Council and Regulation (EC) No 45/2001 of the European Parliament and of the Council. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council should apply as appropriate.

(73) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 14 June 2013.

(74) Since the objective of this Directive, namely to achieve a high common level of security of network and information systems in the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(75) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,

(…)

CHAPTER I

GENERAL PROVISIONS

Article 1. Subject matter and scope

1. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

2. To that end, this Directive:

(a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;

(b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;

(c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;

(d) establishes security and notification requirements for operators of essential services and for digital service providers;

(e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

3. The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.

4. This Directive applies without prejudice to Council Directive 2008/114/EC and Directives 2011/93/EU and 2013/40/EU of the European Parliament and of the Council.

5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where such exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality

of that information and protect the security and commercial interests of operators of essential services and digital service providers.

6. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

7. Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.

Article 2. Processing of personal data
1. Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.

2. Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.

Article 3. Minimum harmonisation
Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.

Article 4. Definitions
For the purposes of this Directive, the following definitions apply:

(1) ‘network and information system ’means:

(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) ‘security of network and information systems ’means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

(3) ‘national strategy on the security of network and information systems ’means a framework providing strategic objectives and priorities on the security of network and information systems at national level;

(4) ‘operator of essential services ’means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);

(5) ‘digital service ’means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council which is of a type listed in Annex III;

(6) ‘digital service provider ’means any legal person that provides a digital service;

(7) ‘incident ’means any event having an actual adverse effect on the security of network and information systems;

(8) ‘incident handling ’means all procedures supporting the detection, analysis and containment of an incident and the response thereto;

(9) ‘risk ’means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

(10) ‘representative ’means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;

(11) ‘standard ’means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;

(12) ‘specification ’means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;

(13) ‘internet exchange point (IXP) ’means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(14) ‘domain name system (DNS) ’means a hierarchical distributed naming system in a network which refers queries for domain names;

(15) ‘DNS service provider ’means an entity which provides DNS services on the internet;

(16) ‘top-level domain name registry ’means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);

(17) ‘online marketplace ’means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

(18) ‘online search engine ’means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

(19) ‘cloud computing service ’means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Article 5. Identification of operators of essential services

1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.

2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

(b) the provision of that service depends on network and information systems; and

(c) an incident would have significant disruptive effects on the provision of that service.

3. For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.

4. For the purposes of paragraph 1, where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.

5. Member States shall, on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.

6. The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of operators of essential services.

7. For the purpose of the review referred to in Article 23 and by 9 November 2018, and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services.

That information shall include at least:

(a) national measures allowing for the identification of operators of essential services;

(b) the list of services referred to in paragraph 3;

(c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector;

(d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1).

In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.

Article 6. Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors:

(a) the number of users relying on the service provided by the entity concerned;

(b) the dependency of other sectors referred to in Annex II on the service provided by that entity;

(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;

(d) the market share of that entity;

(e) the geographic spread with regard to the area that could be affected by an incident;

(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

2. In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors.

CHAPTER II

NATIONAL FRAMEWORKS ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

Article 7. National strategy on the security of network and information systems

1. Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:

(a) the objectives and priorities of the national strategy on the security of network and information systems;

(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;

(c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;

(d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;

(e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;

(f) a risk assessment plan to identify risks;

(g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

2. Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.

3. Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.

Article 8. National competent authorities and single point of contact

1. Each Member State shall designate one or more national competent authorities on the security of network and information systems (‘competent authority’), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.

2. The competent authorities shall monitor the application of this Directive at national level.

3. Each Member State shall designate a national single point of contact on the security of network and information systems (‘single point of contact’). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.

4. The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.

5. Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group.

6. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

7. Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.

Article 9. Computer security incident response teams (CSIRTs)

1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.

2. Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I.

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.

3. Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.

4. Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.

5. Member States may request the assistance of ENISA in developing national CSIRTs.

Article 10. Cooperation at national level

1. Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.

2. Member States shall ensure that either the competent authorities or the CSIRTs receive incident notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6).

3. Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive.

By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).

CHAPTER III

COOPERATION

Article 11. Cooperation Group

1. In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union, a Cooperation Group is hereby established.

The Cooperation Group shall carry out its tasks on the basis of biennial work programmes as referred to in the second subparagraph of paragraph 3.

2. The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA.

Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate in its work.

The Commission shall provide the secretariat.

3. The Cooperation Group shall have the following tasks:

(a) providing strategic guidance for the activities of the CSIRTs network established under Article 12;

(b) exchanging best practice on the exchange of information related to incident notification as referred to in Article 14(3) and (5) and Article 16(3) and (6);

(c) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems;

(d) discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice;

(e) exchanging information and best practice on awareness-raising and training;

(f) exchanging information and best practice on research and development relating to the security of network and information systems;

(g) where relevant, exchanging experiences on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies;

(h) discussing the standards and specifications referred to in Article 19 with representatives from the relevant European standardisation organisations;

(i) collecting best practice information on risks and incidents;

(j) examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10(3);

(k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA;

(l) with ENISA's assistance, exchanging best practice with regard to the identification of operators of essential services by the Member States, including in relation to cross-border dependencies, regarding risks and incidents;

(m) discussing modalities for reporting notifications of incidents as referred to in Articles 14 and 16.

By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the objectives of this Directive.

4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article.

5. The Commission shall adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the committee referred to in Article 22(1) by 9 February 2017.

Article 12. CSIRTs network

1. In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.

2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs.

3. The CSIRTs network shall have the following tasks:

(a) exchanging information on CSIRTs' services, operations and cooperation capabilities;

(b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;

(c) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents;

(d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State;

(e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance;

(f) discussing, exploring and identifying further forms of operational cooperation, including in relation to:

(i) categories of risks and incidents;

(ii) early warnings;

(iii) mutual assistance;

(iv) principles and modalities for coordination, when Member States respond to cross-

border risks and incidents;

(g) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard;

(h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA;

(i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;

(j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.

4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.

5. The CSIRTs network shall lay down its own rules of procedure.

Article 13. International cooperation
The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or inter national organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.

CHAPTER IV

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14. Security requirements and incident notification
1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

(a) the number of users affected by the disruption of the essential service;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident.

5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.

At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.

6. After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

7. Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.

Article 15. Implementation and enforcement

1. Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems.

2. Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide:

(a) the information necessary to assess the security of their network and information systems, including documented security policies;

(b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority.

When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required.

3. Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified.

4. The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.

CHAPTER V

Security of The Network and Information Systems of Digital Service Providers

Article 16. Security requirements and incident notification

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) monitoring, auditing and testing;

(e) compliance with international standards.

2. Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.

3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

(e) the extent of the impact on economic and societal activities.

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

5. Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.

6. Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

7. After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

8. The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017.

9. The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

10. Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.

11. Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC.

Article 17. Implementation and enforcement

1. Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided.

2. For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to:

(a) provide the information necessary to assess the security of their network and information systems, including documented security policies;

(b) remedy any failure to meet the requirements laid down in Article 16.

3. If a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in paragraph 2.

Article 18. Jurisdiction and territoriality

1. For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.

2. A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.

3. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.

CHAPTER VI

STANDARDISATION AND VOLUNTARY NOTIFICATION

Article 19. Standardisation

1. In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

Article 20. Voluntary notification
1. Without prejudice to Article 3, entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

2. When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned.

Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.

CHAPTER VII

FINAL PROVISIONS

Article 21. Penalties
Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

Article 22. Committee procedure
1. The Commission shall be assisted by the Network and Information Systems Security Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 23. Review
1. By 9 May 2019, the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of the approach taken by Member States in the identification of the operators of essential services.

2. The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. In its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by 9 May 2021.

Article 24. Transitional measures
1. Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by 9 February 2017.

2. For the period from 9 February 2017 to 9 November 2018, and for the purposes of supporting Member States in taking a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. The Cooperation Group shall also discuss, at the request of a Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6.

3. By 9 February 2017 and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs network.

Article 25. Transposition

1. Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 10 May 2018.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

(…)

ANNEX I

REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following:

(1) Requirements for CSIRTs:

(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

(b) CSIRTs' premises and the supporting information systems shall be located in secure sites.

(c) Business continuity:

(i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.

(ii) CSIRTs shall be adequately staffed to ensure availability at all times.

(iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.

(d) CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.

(2) CSIRTs' tasks:

(a) CSIRTs' tasks shall include at least the following:

(i) monitoring incidents at a national level;

(ii) providing early warning, alerts, announcements and dissemination of information to

relevant stakeholders about risks and incidents;

(iii) responding to incidents;

(iv) providing dynamic risk and incident analysis and situational awareness;

(v) participating in the CSIRTs network.

(b) CSIRTs shall establish cooperation relationships with the private sector.

(c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:

(i) incident and risk-handling procedures;

(ii) incident, risk and information classification schemes.

ANNEX II

TYPES OF ENTITIES FOR THE PURPOSES OF POINT (4) OF ARTICLE 4

Sector 1. Energy

Subsector (a) Electricity

Type of entity:

- Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council, which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive

- Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC

- Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC

Subsector (b) Oil

Type of entity:

- Operators of oil transmission pipelines

- Operators of oil production, refining and treatment facilities, storage and transmission

Subsector (c) Gas

Type of entity:

- Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council

- Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC

- Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC

- Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC

- LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC

- Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC

- Operators of natural gas refining and treatment facilities

Sector 2. Transport

Subsector (a) Air transport

Type of entity:

- Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council

- Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council, airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council, and entities operating ancillary installations contained within airports

- Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council

Subsector (b) Rail transport

Type of entity:

- Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council

- Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU

Subsector (c) Water transport

Type of entity:

- Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council, not including the individual vessels operated by those companies

- Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council, including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports

- Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council

Subsector (d) Road transport

Type of entity:

- Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 responsible for traffic management control

- Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council

Sector 3. Banking

Type of entity:

- Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council

Sector 4. Financial market infrastructures

Type of entity:
- Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council

- Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council

Sector 5. Health sector

Subsector: Health care settings (including hospitals and private clinics)

Type of entity:

- Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council

Sector 6. Drinking water supply and distribution

Type of entity:

- Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC (17) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services

Sector 7. Digital Infrastructure

Type of entity:

- IXPs

- DNS service providers

- TLD name registries

ANNEX III

TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF POINT (5) OF ARTICLE 4

1. Online marketplace.

2. Online search engine.

3. Cloud computing service.

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of

network and information systems and of the parameters for determining whether an incident has a substantial impact

(…)

Whereas:

(1) In accordance with Directive (EU) 2016/1148, digital service providers remain free to take technical and organisational measures they consider appropriate and proportionate to manage the risk posed to the security of their network and information systems, as long as those measures ensure an appropriate level of security and take into account the elements provided for in that Directive.

(2) When identifying the appropriate and proportionate technical and organisational measures, the digital service provider should approach information security in a systematic way, using a risk-based approach.

(3) In order to ensure the security of systems and facilities, digital service providers should perform assessment and analysis procedures. These activities should concern the systematic management of network and information systems, the physical and environmental security, the security of supplies and the access controls.

(4) When carrying out a risk analysis within the systematic management of network and information systems, digital service providers should be encouraged to identify specific risks and quantify their significance, for example by identifying threats to critical assets and how they may affect the operations, and determining how best to mitigate those threats based on current capabilities and resource requirements.

(5) Policies on human resources could refer to the management of skills, including aspects related to the development of security related skills and awareness-raising. When deciding on an appropriate set of policies on security of operation, the digital service providers should be encouraged to take into account aspects of change management, vulnerability management, formalisation of operating and administrative practices and system mapping.

(6) Policies on security architecture could comprise in particular the segregation of networks and systems as well as specific security measures for critical operations such as administration operations. The segregation of networks and systems could enable a digital service provider to distinguish between elements such as data flows and computing resources that belong to a client, group of clients, the digital service provider or third parties.

(7) The measures taken with regard to the physical and environmental security should ensure the security of an organisation's network and information systems from damage caused by incidents such as theft, fire, flood or other weather effects, telecommunications or power failures.

(8) The security of supplies such as electrical power, fuel or cooling could encompass the security of the supply chain that includes in particular the security of third party contractors and subcontractors and their management. The traceability of critical supplies refers to the ability of the digital service provider to identify and record sources of those supplies.

(9) The users of digital services should encompass natural and legal persons who are customers of or are subscribers to an online marketplace or a cloud computing service, or who are visitors to an online search engine website in order to undertake keyword searches.

(10) When defining the substantiality of the impact of an incident, the cases laid down in this regulation should be considered as a non-exhaustive list of substantial incidents. Lessons should be drawn from the implementation of this Regulation and from the work of the Cooperation Group as regards the collection of best practice information on risks and incidents and the discussions on modalities for reporting notifications of incidents as referred to in points (i) and (m) of Article

11(3) of Directive (EU) 2016/1148. The result could be comprehensive guidelines on quantitative thresholds of notification parameters that may trigger the notification obligation for digital service providers under Article 16(3) of Directive (EU) 2016/1148. Where appropriate, the Commission could also consider reviewing the thresholds currently laid down in this Regulation.

(11) In order to enable competent authorities to be informed about potential new risks, the digital service providers should be encouraged to voluntarily report any incident whose characteristics have been previously unknown to them such as new exploits, attack-vectors or threat actor, vulnerabilities and hazards.

(12) This Regulation should apply on the day following the expiry of the deadline for transposition of Directive (EU) 2016/1148.

(13) The measures provided for in this Regulation are in accordance with the opinion of the Network and Information Systems Security Committee referred to Article 22 of Directive (EU) 2016/1148,

(…)

Article 1. Subject matter
This Regulation specifies further the elements to be taken into account by digital service providers when identifying and taking measures to ensure a level of security of network and information systems which they use in the context of offering services referred to in Annex III to Directive (EU) 2016/1148 and specifies further the parameters to be taken into account to determine whether an incident has a substantial impact on the provision of those services.

Article 2. Security elements
1. Security of systems and facilities referred to in point (a) of Article 16(1) of Directive (EU) 2016/1148 means the security of network and information systems and of their physical environment and shall include the following elements:

(a) the systematic management of network and information systems, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management;

(b) physical and environmental security, which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an all-hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena;

(c) the security of supplies, which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and where applicable the traceability of critical supplies used in the provision of the services;

(d) the access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including administrative security of network and information systems, is authorised and restricted based on business and security requirements.

2. With regard to incident handling referred to in point (b) of Article 16(1) of Directive (EU) 2016/1148, the measures taken by the digital service provider shall include:

(a) detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;

(b) processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems;

(c) a response in accordance with established procedures and reporting the results of the measure taken;

(d) an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.

3. Business continuity management referred to in point (c) of Article 16(1) of Directive (EU) 2016/1148 means the capability of an organisation to maintain or as appropriate restore the delivery of services at acceptable predefined levels following a disruptive incident and shall include:

(a) the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by digital service providers which shall be assessed and tested on a regular basis for example, through exercises;

(b) disaster recovery capabilities which shall be assessed and tested on a regular basis for example, through exercises.

4. The monitoring, auditing and testing referred to in point (d) of Article 16(1) of Directive (EU) 2016/1148 shall include the establishment and maintenance of policies on:

(a) the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;

(b) inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;

(c) a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.

5. International standards referred to in point (e) of Article 16(1) of Directive (EU) 2016/1148 mean standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council (1). Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

6. Digital service providers shall ensure that they have adequate documentation available to enable the competent authority to verify compliance with the security elements set out in paragraphs 1, 2, 3, 4 and 5.

Article 3. Parameters to be taken into account to determine whether the impact of an incident is substantial

1. With regard to the number of users affected by an incident, in particular users relying on the service for the provision of their own services referred to in point (a) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be in a position to estimate either of the following:

(a) the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or

(b) the number of affected users having used the service based in particular on previous traffic data.

2. The duration of an incident referred to in point (b) of Article 16(4) means the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.

3. As far as the geographical spread with regard to the area affected by the incident referred to in point (c) of Article 16(4) of Directive (EU) 2016/1148 is concerned, the digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States.

4. The extent of disruption of the functioning of the service referred to in point (d) of Article 16(4) of Directive (EU) 2016/1148 shall be measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.

5. With regard to the extent of the impact on economic and societal activities referred to in point (e) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be able to conclude, based on indications such as the nature of his contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety or damage to property.

6. For the purpose of paragraph 1, 2, 3, 4 and 5, the digital service providers shall not be required to collect additional information to which they do not have access.

Article 4. Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

(a) the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;

(b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;

(c) the incident has created a risk to public safety, public security or of loss of life;

(d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

2. Drawing on the best practice collected by the Cooperation Group in the exercise of its tasks under Article 11(3) of Directive (EU) 2016/1148 and on the discussions under point (m) of Article 11(3) thereof, the Commission may review the thresholds laid down in paragraph 1.

(...)

See also: Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union

COMMUNICATION from the Commission to the European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (COM(2017) 476 final/2)

Introduction

The Directive (EU) 2016/1148 on the security of network and information systems across the Union (hereinafter referred to as "NIS Directive" or the "Directive") adopted on 6 July, 2016 is the first EU horizontal legislation addressing cybersecurity challenges and a true game changer for cybersecurity resilience and cooperation in Europe.

The Directive has three main objectives:

- Improving national cybersecurity capabilities;

- Building cooperation at EU level; and

- Promoting a culture of risk management and incident reporting among key economic actors, notably operators providing essential services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSPs).

The NIS Directive is a cornerstone of the EU's response to the growing cyber threats and challenges which are accompanying the digitalisation of our economic and societal life, and its implementation is therefore an essential part of the cybersecurity package presented on 13 September, 2017. The effectiveness of the EU's response is inhibited as long as the NIS Directive is not fully transposed in all EU Member States. This was also recognized as a critical point in the Commission's 2016 Communication on Strengthening Europe's Cyber Resilience System.

The novelty of the NIS Directive and the urgency of tackling a fast evolving cyber-threat landscape warrant particular attention to the challenges faced by all actors in ensuring the timely and successful transposition of the Directive. In view of the transposition deadline of 9 May, 2018, and the deadline for the identification of operators of essential services of 9 November, 2018, the Commission has been supporting the Member States 'transposition process and their work in the Cooperation Group to this end.

The present Communication with its annex is based on the Commission's preparatory work and analysis related to the implementation of the NIS Directive thus far, on the input of the European Agency for Network and Information Security (ENISA) and on the discussions held with Member States in the transposition phase of the Directive, notably within the Cooperation Group. This Communication complements the considerable efforts taken so far, in particular through:

- The intensive work of the Cooperation Group, which has agreed to a working plan focusing predominantly on the transposition of the NIS Directive, and in particular on the question of identification of operators of essential services and their obligations concerning security requirements and incident notifications. While the Directive provides for discretion in transposing provisions related to operators of the essential services, Member States recognised the importance of a harmonised approach in this respect .

- The establishment and swift operation of the Network composed of Computer Security Incident Response Teams (CSIRTs) in accordance with Article 12(1) of the Directive. Since then, this network has started to lay the foundations for structured operational cooperation at European level.

For both the policy and the operational levels represented by these two structures, the full engagement of all Member States is essential to achieve the goal of a high common level of security of network and information systems in the Union.

The present Communication with its annex will reinforce these efforts by bringing together and comparing best practices from the Member States which are relevant for the implementation of the Directive, by providing further guidance on how the Directive should be implemented and through more detailed explanations on specific provisions. The overarching goal is to support Members States to achieve an effective and harmonised implementation of the NIS Directive across the EU.

This Communication will be further complemented by the upcoming Commission's Implementing Regulation on further specification of elements and parameters related to the security and incident notification requirements for digital service providers, pursuant to Article 16(8) of the NIS Directive. The Implementing Regulation will facilitate the implementation of the Directive with respect to obligations concerning digital service providers.

The Communication presents the key conclusions of the analysis of the issues which are seen as important points of reference and potential inspiration from the point of view of the transposition into national law. Here the primary focus is on provisions related to Member States 'capabilities and obligations concerning entities that are within the scope of the Directive. The annex provides a more detailed examination of those areas where the Commission sees the greatest value in providing practical transposition guidance through the explanation and its interpretation of certain Directive's provisions, and through presentation of best practices and accumulated experience with the Directive so far.

Towards the effective implementation of the NIS Directive

The objective of the NIS Directive is to achieve a high common level of security of network and information systems within the EU. This means improving the security of the Internet and private networks and information systems underpinning the functioning of our society and economy. The first important element in this regard is the Member States 'preparedness which should be ensured by having national cybersecurity strategies in place, as described in the Directive, by the work of the CSIRTS, and by that of the competent national authorities.

Comprehensiveness of national strategies

It is important that Member States seize the opportunity of the transposition of the NIS Directive to review their national cybersecurity strategy in the light of the gaps, best practices and new challenges addressed in the Annex.

While the Directive understandably focuses on those companies and services that are of particular critical importance, it is the cybersecurity of the economy and society as a whole that needs to be addressed in a wholistic and consistent manner, given the ever increasing reliance on ICT. Therefore, the adoption of comprehensive national strategies which go beyond the minimum requirements of the NIS Directive (i.e. covering more than the sectors and services listed respectively in the Directive's Annex II and III) would increase the overall level of security of network and information systems.

As cybersecurity is still a relatively new and rapidly expanding area of public policy, new investments are required in most cases, even if the overall situation in public finances calls for cuts and savings. Taking ambitious decisions to secure adequate financial and human resources which are indispensable for the effective implementation of national strategies, including the sufficient resourcing of national competent authorities and CSIRTs, is therefore fundamental for the achievement of Directive's objectives.

Effectiveness of implementation and enforcement

The need to designate respective national competent authorities and single points of contacts is outlined in the Directive's Article 8 and is a key element to ensure an effective implementation of the NIS Directive and cross-border cooperation. Here both more centralised and decentralised approaches have emerged in Member States. When Member States adopt a more decentralised approach with regard to the designation of national competent authorities, ensuring strong cooperative arrangements between numerous authorities and the single point of contact has proved to be of essence (see Table 1 of section 3.2. of the Annex). This would increase effectiveness of implementation and facilitate enforcement.

Drawing on previous experience in relation to Critical Information Infrastructure Protection (CIIP) may help to design an optimal model of governance for Member States, ensuring both effective sectoral implementation of the NIS Directive, as well as a coherent horizontal approach (see section 3.1. of the Annex).

Enhanced national CSIRTs' capabilities

Without effective and adequately resourced national CSIRTs across the EU, as laid out in Article 9 of the NIS Directive, the EU will remain too vulnerable to cross-border cyber threats. Member States could therefore consider extending the scope of CSIRTs beyond sectors and services that are included in the scope of the Directive (see section 3.3 of the Annex). This would enable national CSIRTs to provide operational support to cyber incidents that occur in companies and organisations which are not in the scope of the Directive but are also important for the society and economy. In addition, Member States could make full use of additional funding opportunities offered by the Cybersecurity Digital Service Infrastructures (DSI) programme of the Connecting Europe Facility (CEF), designed to enhance capabilities of national CSIRTs and cooperation among them (see section 3.5 of the Annex).

Consistency of the identification process of OES

In accordance with Article 5 of the NIS Directive Member States are required to identify the entities that will be considered operators of essential services by 9 November, 2018. In relation to this task, Member States could consider using consistently the definitions and guidance included in this Communication in order to ensure that similar type of entities playing a similar role in the internal market would consistently be identified as operators of essential services in other Member States. Member States could also consider extending the scope of the NIS Directive to public administrations, given the role they play for society and the economy as a whole (see sections 2.1. and 4.1.3 of the Annex).

Aligning national approaches to the identification of operators of essential services to a maximum extent, notably by following guidance developed by the Cooperation Group (see section 4.1.2 of the Annex) would be very useful, as it would lead to a more harmonised application of the Directive's provisions and thus reduce the risk of market fragmentation. In cases where operators of essential services provide essential services in two or more Member States, striving to reach an agreement between Member States in the context of the consultation process under Article 5(4)) on the consistent identification of entities, (see section 4.1.7 of the Annex) is essential, as this would avoid a different regulatory treatment of the same entity under different Member State jurisdictions.

Submission of information on identification of OES to the Commission

In accordance with Article 5(7), Member States are requested to provide to the Commission information on national measures allowing for the identification of OES, the list of essential services, the number of identified OES and the relevance of those operators for the sector. Furthermore, Member States are requested to provide thresholds, where such exist, used in the identification process to determine the relevant supply level or the importance of the particular

operator for maintaining a sufficient level of supply. Member States could also consider sharing with the Commission the lists of identified operators of essential services and if necessary on a confidential basis, as this would help to improve the accuracy and quality of the Commission's assessment (see sections 4.1.5. and 4.1.6. of the Annex).

Aligned approaches concerning security and incident notification requirements for OES

In relation to obligations concerning security requirements and incident notifications for operators of essential services (Article 14(1), (2) and (3)), an aligned approach regarding the security requirements and incident notifications in order to facilitate the compliance of OESs across EU Member State borders, would promote to the greatest extent possible a single market effect. The reference here remains the work on a guidance document within the Cooperation Group (see sections 4.2. and 4.3. of the Annex).

In case of a large scale cyber incident affecting several Member States, it is very likely that a mandatory incident notification is submitted by an OES or DSP pursuant to article 14(3) and 16(3) or by another entity which is not in the scope of the Directive on a voluntary basis pursuant to article 20(1). In line with the Commission Recommendation on Coordinated Response for Large-Scale Cybersecurity incidents and crises, Member States could consider aligning their national approaches so that they can provide as soon as possible, relevant information based on those notifications to the competent authorities or the CSIRT of other Member States concerned. Accurate and actionable information would be vital for reducing the number of infections or addressing vulnerabilities before they are exploited.

In the spirit of partnership in making the most from the NIS Directive, the Commission intends to extend support under the Connecting Europe Facility to all relevant stakeholders under this legislation. While the focus has been on CSIRT capacity building and on an enabling platform for swift and effective operational co-operation, thereby re-enforcing the CSIRT Network, the Commission will now explore how funding under Connecting Europe Facility can also benefit national competent authorities as well as operators of essential services and digital service providers.

Conclusion

In view of the impending deadline for the transposition of the NIS Directive into national legislation by 9 May, 2018, and in view of the deadline for the identification of operators of essential services by 9 November, 2018, Member States should take appropriate measures to ensure that the provisions and the cooperation models of the NIS Directive can provide the best possible EU-level tools to achieve a high common level of security of network and information systems across the Union. The Commission invites Member States to consider in this process the relevant information, guidance and recommendations contained in this Communication.

This Communication may be further supplemented by other actions, including those generated through ongoing work within the framework of the Cooperation Group.

(...)

ANNEX

1. Introduction.

This Annex aims to contribute to an effective application, implementation and enforcement of the NIS Directive (EU) 2016/1148 on the security of network and information systems across the Union (hereinafter referred to as "NIS Directive" or the "Directive") and to help the Member States to ensure that EU law is applied effectively. More particularly, its specific objectives are threefold: (a) to offer greater clarity to national authorities on the obligations contained in the Directive that

apply to such authorities, (b) to ensure the effective enforcement of the Directive's obligations applying to entities under obligations concerning security requirements and incident notifications, and (c) to overall contribute to create legal certainty for all relevant actors.

To this end, this Annex provides guidance on the following aspects, which are key to achieve the goal of the NIS Directive i.e., to ensure a high common level of security of network and information systems within the EU, underpinning the functioning of our society and economy:

- Member States 'obligation to adopt a national strategy on security of network and information systems (section 2);

- The setting up of national competent authorities, single contact points and Computer Security Incident Response Teams (section 3);

- The security and incident notifications requirements applicable to operators of essential services and to digital service providers (section 4); and

- The relationship between the NIS Directive and other legislation (section 5)

To prepare this guidance, the Commission has used input and analysis gathered during the preparation of the Directive, input from European Agency for network and information security ("ENISA") and Cooperation Group. It has also used experiences from specific Member States. When appropriate, the Commission has taken into account the guiding principles for interpreting EU law: the wording, context and objectives of the NIS Directive. Given that the Directive has not been transposed, no ruling of the Court of Justice of the European Union (CJEU) or national courts has yet been rendered. Therefore, it is not possible to use case-law as guidance.

Compiling this information in a single document may allow Member States to have a good overview of the Directive and take this information into account when devising their national legislation. At the same time, the Commission stresses that this Annex is not binding and does not intend to create new rules. The final competence to interpret EU law lies with the CJEU.

(…)

Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems (COM/2019/546 final)

(…)

3. Conclusions

This report evaluates the approaches chosen by Member States to identify operators of essential services (OES) under the NIS Directive. Its goal is to assess the level of consistency between the practices of Member States in view of the possible impact of the current framework on the functioning of the internal market and the management of the risks associated with cyber-dependence.

The analysis conducted shows that the NIS Directive has served as catalyst in many Member States paving the way for real change in the institutional and regulatory landscape with regard to cyber-security. In addition, the obligation to identify operators of essential services has triggered a comprehensive assessment of the risks associated with operators active in critical activities and modern network and information systems in almost all the Member States. This can be considered an achievement for the Union as a whole in line with the objectives of the Directive.

For the purpose of this report, the Commission has examined the national identification methodologies, the services national authorities deem as essential, the identification thresholds, and the numbers of OES identified in the various sectors covered by the Directive:

- Member States have developed a variety of methodologies when it comes to the overall approach to the identification of OES (section 2.1) but also regarding the definition of essential services and the setting of thresholds. This can have a negative impact on the consistent application of the NIS provisions across the Union with possible consequences for the well-functioning of the internal market and the effective handling of cyber-dependencies.

- In addition, it seems that there are diverging interpretations by Member States as to what constitutes an essential service under the NIS Directive, with Member States applying different levels of granularity (see section 2.2). This makes it difficult to compare the lists of essential services. In addition, the scope of the Directive risks being fragmented, with some operators being exposed to additional regulation (because they have been identified by their respective Member State) while others providing similar services remaining excluded (because they have not been identified). In order to address these inconsistencies, further work based on the experience of Member States could lead to a more aligned list of essential services.

- Moreover, the report has also found significant inconsistencies in the way thresholds are applied by Member States (section 2.3). A further alignment of thresholds on EU level could help alleviate this problem. Such work could for example be undertaken by sectoral work streams under the Cooperation Group, taking into account national specificities, such as the special requirements of small Member States.

- The fact that some countries have made use of the possibility to identify essential services in additional sectors or subsectors beyond those covered by Annex II highlights that there are other sectors potentially vulnerable to cyber-incidents than considered by the NIS Directive (section 2.5). The identification of OES in sectors, such as information infrastructures, financial services not covered by entities listed in Annex II and government can improve the cyber-resilience of organisations in such sectors. However, if only a subset of Member States identifies OES in such sectors, this could have negative consequences for the internal market and the level playing field, which it is supposed to ensure.

The many methodologies and best practices that national authorities have devised are of particular value and should be taken into account in the future, for example in the work of the Cooperation Group and the continuous identification of OES by Member States. However, the current level of diversity could have a negative impact on achieving the Directive's goals.

The Commission draws the preliminary conclusion that, while the NIS Directive has set into motion a crucial process to increase and improve risk management practices of operators in critical sectors, there is a considerable degree of fragmentation across the Union when it comes to the identification of OES. This is partly due to the design of the Directive and partly due to the different implementation methodologies used by the Member States.

Member States should seek to apply the provisions of the NIS Directive in a manner as consistent as possible, making full use of guidance documents developed by the Commission and the Cooperation Group. The Commission has therefore identified several national actions that could help alleviate the problems highlighted in this report:

- Many Member States have not completed the OES identification process within the timeframe set by the Directive. Moreover, on the date of publication of this report 23 Member States had submitted all the data required under Article 5(7). An additional 5 Member States had provided partial information. The Commission urges the national authorities in charge of identification to complete the process as quickly as possible and to transmit the information necessary to the Commission in the shortest delay.

- Competent authorities should regularly review their lists of essential services and ensure that all existing essential services are identified so that the number of "consistency gaps" regarding essential services across the internal market is reduced.

- Member States should more actively engage with each other in order to align thresholds where possible and especially in sectors with a strong cross-border dimension, such as transport or energy. This can be achieved via the cross-border consultation procedure provided for in Article 5(4) of the NIS Directive but also by making better use of the existing structures of the Cooperation Group.

- National authorities should consult each other in order to ensure that cross-border operators face similar security and incident reporting requirements in the internal market. Moreover, Member States should contact such operators to gather more information about regulatory divergence. Enhanced cyber-resilience should not come at the cost of regulatory fragmentation. Where necessary, Member States should also engage in multilateral discussions, as envisaged by Recital 24 of the NIS Directive.

In addition to national actions, there are a number of measures that could potentially be taken at Union level and that would lead to increased consistency. The Commission will launch discussions to improve the uneven and at times fragmented identification landscape. Some of the potential measures are:

- The role of the NIS Cooperation Group should be strengthened in order to promote a common understanding on how to implement the Directive in a more consistent manner. For this purpose, the Commission will propose that the existing dedicated work stream on identification of OES reviews swiftly its guidelines to better tackle existing inconsistencies. The Cooperation Group should also explore the creation of additional sectoral work streams with a view to increasing coherence between Member States and the use of a tailor-made communication tool to enhance collaboration within the group.

- Only very few Member States are currently making use of the cross-border consultation procedure when it comes to identifying operators that are providing essential services in more than one Member State. In order to enhance the exchange of information, the Cooperation Group should review its reference document on the modalities of the consultation process in cases with cross-border impact and agree on a consistent interpretation of the scope, objectives and procedures of such exercise. At the same time, the Commission will look into ways allowing for a secure exchange of information between competent authorities.

- There appears to be a certain degree of inconsistency in the application of the provisions of the Directive on lex specialis amongst Member States. The Commission will therefore make use of the structures of the Cooperation Group to discuss cases where the application of the lex specialis principle may not be correct.

Actions taken at Union level should guarantee a coherent framework, taking into account both sectoral activities envisaging specific or higher requirements on cyber-security and other European legislation.

(…)

NIS Cooperation Group Publications

1.10 Reference document on security measures for Operators of Essential Services (CG Publication 01/2018)

1. Introduction

Background
Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures

for a high common level of security of network and information systems across the Union (hereinafter: "NIS Directive") was adopted on 6 July 2016.

Laying down "measures with a view to achieving a high common level of security of network and information systems within the EU" the NIS Directive in particular provides with measures aimed at improving the cybersecurity of operators considered "essential for the maintenance of critical societal and/or economic activities".

Public or private entities providing services "essential to the maintenance of critical societal and/or economic activities", these "Operators of Essential Services" (OES) shall be identified by each Member State on its territory and comply with several binding provisions defined nationally.

In particular, "Member States shall ensure that OES take appropriate and proportionate technical and organisational security measures to manage risks posed to the security of NIS they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed".

Furthermore "Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of (...) essential services, with a view to ensuring the continuity of those services".

Individually responsible for the transposition of these provisions into National law, Member States may moreover adopt or maintain provisions with a view to achieving a higher level of security of network and information systems, according the principle of minimum harmonisation set in the Directive.

Nevertheless, with a view of fostering mutual understanding of challenges related to the implementation of key provisions of the Directive and of supporting convergence of national approaches to their implementation, a Cooperation Group (CG) is established to facilitate exchange of information and best practices among Member States.

Taking advantage of this possibility and upon proposal from the European Commission (EC) a group of voluntary Member States 'experts (hereinafter: "the Group") was therefore established within the framework of the Cooperation Group with the support of ENISA, in view of exchanging views on the issue of security measures for OES.

The present "reference document" provides with a summary of the Group's main findings.

This panorama doesn't aim at establishing a new standard nor to duplicate existing ones (e.g. ISO) but to provide Member States with a clear and structured picture of Member States 'current and often common approaches to the security measures of OES.

Beyond OES, this reference document providing with indications on domains of cybersecurity measures may be considered useful by other public or private actors in improving their cybersecurity.

Purpose

Cyberthreats to critical infrastructures are now recognized as among the most serious threats to the EU, its Member States, the economy and the society.

Essential to the functioning of the Single Market, due to their contribution to critical economic and societal functions such as in the fields of Energy, Transport or Banking, OES are indeed targets of choice. Malicious actors, constantly developing their tools and techniques often advanced and

targeting the weakest may indeed choose to target OES and thus harm the critical functions supporting our economy and society.

By requiring OES to comply with "appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems", the NIS Directive aimed at significantly raising the level of security of OES in view of allowing them to face the serious risks posed to the security of their critical information systems supporting their essential operations.

Reinforcing OES 'cybersecurity will therefore significantly contribute to reducing the risks to the EU and Member States 'cybersecurity.

Recognizing the solid and growing risk posed to OES and their potential impact on EU's economy and society and taking into account that some OES may be established in different EU Member States, the Group agreed that all may benefit from indications towards more coherent approaches to the transposition of the NIS Directive with regard to security measures for OES foreseen in article 14 (1) and (2).

Outcome

Building upon answers provided by the Member States ENISA's questionnaire, the Group acknowledged that Member States may wish to

- Use different sources or control frameworks for security measures from European or International standards (e.g. ISO 27.000) to existing or new sets of security measures (e.g. France's cybersecurity measures for OES, Germany's IT-Grundschutz, Spain's National Security Framework, etc.).

- Aim at different levels of granularity and prescription regarding specific cybersecurity requirements, objectives and controls.

- Aim to only establish cross-sectoral measures or choose to address individual sector specificities as well (with sector-specific measures).

Nevertheless, despite those differences, the Group agreed that a common consensual basis could be identified in view of fostering convergence of national approaches to the transposition of the Directive.

Thus, the Group managed draw an inclusive picture of Member States 'existing and often common approaches regarding principles and domains of cybersecurity measures which should enlighten the national transposition of OES 'security measures related provisions.

2. Principles

Despite different possible approaches to the national transposition of article 14 (1) and (2) of the NIS Directive on security measures for OES, the Group agreed that Member States should take the utmost into account the following general principles.

First, security measures should be:

- Effective in view significantly increasing the cybersecurity of OES, in relation to the current and foreseen threat landscape described above.

- Tailored in view of putting OES 'efforts on measures having the most impact on their cybersecurity and avoid unnecessary effort and duplication.

- Compatible in view of addressing, on the short term, basic and common security vulnerabilities of OES despite their sectors, which may in the meantime be complemented with sector specific security measures;

- Proportionate to the risks, in view of avoiding unnecessary burden for OES, for instance by privileging applying security measures only to the critical information systems underlying the OES 'information systems operating their essential services.

- Concrete and easy to apprehend, to ensure that the security measures are actually implemented by OES and actually contribute to reinforcing their cybersecurity.

- Verifiable, to ensure that operators may provide to their national NIS competent authority(ies) "evidence of the effective implementation of security policies, such as results of a security audit carried out by the competent authority or a qualified auditor"7.

- Inclusive, to encompass all security domains which may contribute to reinforcing the cybersecurity of OES, including physical security of information systems.

Beyond these principles, Member States should:

- Acknowledge the added-value of dialogue with public and private operators, in particular with regard to the implementation of the security measures. Member States should consider establishing Public and Private Partnerships with OES. Such PPPs may be used in view of

- identifying relevant cross-sectoral or sectoral measures which could be adopted, taking into account the above mentioned principles and the list of suggested cybersecurity measures ' domains (below);

- establishing a permanent dialogue with OES to facilitate the implementation of these measures.

- Find a proper cost-benefit balance so that to ensure efficient security measures, with respect to the security of essential services to the economy and the society, while taking into account their cost for OES'.

3. Domains of cybersecurity measures

(...)

PART 1 - GOVERNANCE AND ECOSYSTEM

1.1 Information System Security Governance & Risk Management

Information system security risk analysis,

The operator conducts and regularly updates a risk analysis, identifying its Critical Information Systems (CIS) underpinning the provision of the essential services of OES and identifies the main risks to these CIS. This process is essential to build and maintain a robust risk management organization. The results of the updates should be implemented through a virtuous circle of continuous improvement.

The risk assessment takes into account, in particular:

- new threats

- recently discovered weaknesses

- loss of effectiveness of measures

- changes to the risk situation caused by changes to the system architecture

- any other changes in the risk situation

Information system security policy

Building upon the risks analysis, the operator establishes, maintains up-to-date and implements an information system security policy (ISSP) and an information security management system (ISMS) approved by senior management, guaranteeing high level endorsement of the policy.

The policy sets out strategic security objectives, describes the security governance (or risk management organization), and refers to all relevant specific information system security policies (e.g. on the security accreditation process, security audit, cryptography, security maintenance, incident handling, etc.).

Information system security accreditation

Building on the risk analysis and according to an accreditation process referred to in the ISSP, the operator accredits itself CIS identified in its information system risk analysis, including inter alia the inventory and architecture of the administration components of the CIS.

Here the "accreditation of CIS" should be understood as the decision by the Operator himself identifying its CIS, the risks associated and the residual risks that the Operator chooses to accept.

The purposes of the accreditation process for the operator are to integrate the CIS within the risk management organization and to formally accept the residual risks.

As part of the accreditation process and depending on the risks analysis, a security audit of the CIS should be carried out. That audit should aim at checking the application and effectiveness of the security measures that apply to the CIS.

The CIS accreditation decision should take into account the risk analysis, the security measures applied to the CIS, audit reports and the residual risks, and the reasons to justify their acceptance.

The operator maintains an up-to-date map of its CIS.

Information system security indicators

For each CIS and according to a number of indicators and assessment methods, the operator evaluates its compliance with its ISSP. Indicators may relate to the risk management organization's performance, the maintaining of resources in secure conditions, users 'access rights, authenticating access to resources, and resource administration.

Information system security audit

The operator establishes and updates a policy and procedures for performing information system security assessments and audits of critical assets and CIS, taking into account the regularly updated risks analysis.

Human resource security

The operator ensures that, first, employees and contractors understand and demonstrate their responsibilities and are suitable for the roles for which they are considered and, second, commit to their roles.

The established information system security policies sets up a CIS security awareness raising program for all staff and a security training program for employees with CIS related responsibilities.

Asset management

The operator sets a suitable framework for identifying, classifying and implementing an inventory of the IT-processes, systems and components of the CIS. This asset management supports the rollout of updates and patches and where appropriate determines, which components are affected by new security issues.

1.2 Ecosystem management

Ecosystem mapping

The operator establishes a mapping of its ecosystem, including internal and external stakeholders, including but not limited to suppliers, in particular those with access to or managing operator's critical assets.

The purpose of this mapping is to identify and evaluate the potential risks represented by the relations with the stakeholders of the ecosystem. To perform this evaluation, the operator might consider four major parameters:

- Maturity: what are the stakeholder's technical capabilities regarding cybersecurity?

- Trust: Can I assume that the stakeholder's intentions toward me are reliable?

- Access level: What are the stakeholder's access rights to my critical assets and CIS?

- Dependence: To which extent is the relationship with my stakeholders critical to my activity?

Ecosystem relations

The operator establishes a policy towards its relations with its ecosystem in order to mitigate the potential risks identified. This includes in particular interfaces between the CIS and third parties. Generally, security requirements must been taken into account for CIS-components operated by third parties. The operator ensures via service level agreements (SLA) and/or auditing mechanisms that his suppliers also establish adequate security measures.

PART 2 - PROTECTION

2.1 IT Security Architecture

Systems configuration

The operator only installs services and functionalities or connects equipment which are essential for the functioning and the security of its CIS. If additional components are unavoidable (e.g. for economic reasons), they are analyzed according to the risk analysis. Those components should only be used to the necessary extent and with adequate security measures.

For example, the operator only connects to its CIS equipment, hardware peripheral and removable media that it has duly itemized and that are essential for the functioning or the security of its CIS.

System segregation

The operator segregates its systems in order to limit the propagation of IT security incidents within its systems or subsystems.

To this aim, the operator segregates physically or logically each CIS from the operator's other information systems or from third party information system. In the case a CIS itself is composed of subsystems, the operator segregates these last physically or logically. The operator allows only interconnections - between CIS and other systems or between CIS subsystems - that are essential for the functioning and security of a CIS.

The operator implements adequate security measures for unavoidable interfaces (e.g. interfaces to the IT of suppliers or customers).

Traffic filtering

The operator filters traffic flows circulating in its Critical Information Systems (CIS). The operator therefore forbids traffic flows that are not needed for the functioning of its systems and that are likely to facilitate an attack.

The operator defines and regularly updates the filtering rules (by network address, by port number, by protocol, etc.) in order to restrain traffic flows to flows needed for the functioning and the security of the CIS.

The operator filters flows entering and existing CIS and flows between CIS subsystems at the level of their interconnection, therefore limiting the flows strictly necessary for the functioning and security of CIS.

Cryptography

In its ISSP, the operator establishes and implements a policy and procedures related to cryptography, in view of ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information in its CIS.

2.2 IT Security Administration

Administration accounts

The operator sets up specific accounts for the administration, to be used only for administrators that are carrying out administration operations (installation, configuration, management, maintenance, etc.) on its CIS. These accounts are kept on an up-to-date list, which can be done for non-administration accounts as well.

To this aim, the permissions given to administrators are individualized and restricted as much as possible to the functional and technical perimeter of each administrator. The administrator accounts are only used to connect to administration information system. While these accounts are used for administration purposes only, administration operations are realized exclusively with the use of administrator accounts.

Administration information systems

Hardware and software resources used for administration purposes are managed and configured by the operator, or, where appropriate, by the service provider that the operator has authorised to carry out administration operations.

Administration information systems used for administration purposes only and to carry out administration operations and should not be mixed up with other operations. In particular administration accounts 'software environment is not used for access to web sites or messaging systems on the internet, and users do not connect to a system used for administration purposes through a software environment used for other functions than administration operations.

The operator sets up a dedicated physical network to connect administration systems to the resources to be administered. The administrator uses to this purpose the resources 'physical administration interface.

In case administration measures are not conducted through the dedicated network, administration flows are protected by authentication and encryption mechanisms.

No password, in form of plain text or hash is written in the logs recording events produced by the resources used for administration, or stored in such form at any time whatsoever.

2.3 Identity and access management

Authentication and identification

For identification, the operator sets up unique accounts for users or for automated processes that need to access resources of its CIS. Unused or no longer needed accounts are to be deactivated. A regular review process should be established.

For authentication, the operator protects access to resources of its CIS for users or automated processes using authentication mechanism. The operator defines the rules for the management of authentication credentials of its CIS.

Whenever this is necessary, and in cases this is feasible, the operator should change authentication credentials. In particular, the operator should change from start the default authentication credentials installed by the manufacturer/supplier of a resource before that resource goes into operation. Neglecting this aspect would pose a high risk to the security of any infrastructure that such a resource is a part of or interacts with.

Access rights

Among the rules defined in its systems security policy, the operator grants access rights to a user or an automated process only when that access is strictly necessary for the user to carry out their mission or for the automated process to carry out its technical operations. The principles of need to know and least privilege should be applied.

The operator defines access rights to the multiple functionalities of the resource, and allocates those access rights strictly to users / automated processes with a clear necessity. The operator reviews at least yearly these access rights, covering the links between accounts, associated access rights, and the resources or functionalities that are accessed with those access rights, and keep an updated list of privileged accounts (e.g. an administration account). The operator checks any potential modification to a privileged account to verify that access rights to resources and functionalities are allocated based on the principle of least privilege (only the rights that are strictly necessary are granted), and are adequate with the usage of the account.

2.4 IT Security Maintenance

IT security maintenance procedure

The operator develops and implements a procedure for security maintenance in accordance with its ISSP. To this purpose, the procedure defines the conditions enabling the minimum security level to be maintained for CIS resources. The procedure, which describes the policy on installing any new version or corrective measure for a designated resource, also states the operator's self-obligation of information on vulnerabilities and corrective security measures that concern CIS resources (hardware and software).

The operator installs and maintains only versions of their CIS hardware and software resources that are supported by their suppliers or manufacturers and up to date from a security point of view. The operator checks the origin and integrity of the version before its installation (as per the timescales defined in the procedure), and analyse the technical and operational impact of that version on the CIS concerned.

The operator protects access to its CIS when access is made through third party networks. In this case, the operator protects by encryption and authentication mechanisms access to the CIS as well as the mass storage of equipments used to access the CIS, and also manages and configures the above mentioned equipments.

Industrial control systems

Many essential services depend on functioning and secure industrial control systems (ICS). If applicable, the operator takes the particular security requirements for ICS into account. For

example, the classical information technology approach (which is focused on transfer of and access to information) could be replaced by an operational technology approach (hardware and software is used to cause or detect changes in a physical process).

2.5 Physical and environmental security

The operator prevents unauthorized physical access, damage and interference to the organization's information and information processing facilities.

PART 3 - DEFENSE

3.1 Detection

Detection

The operator sets up a security incident detection system of the "analysis probe for files and protocols" type. The analysis probes for files and protocols analyses the data flows transiting through those probes in order to seek out events likely to affect the security of CIS. They are positioned so that they can analyse all flows exchanged between the CIS and third-party information systems.

Logging

The operator sets up a logging system on each CIS in order to record events relating, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the CIS and which covers application servers that support critical activities; system infrastructure servers; network infrastructure servers; security equipments; engineering and maintenance stations of industrial systems; network equipments; administrative workstations. The operator records through the logging system events with time and date-stamping using synchronised time sources and centralises archives for at least half-a-year.

Logs correlation and analysis

The operator creates a log correlation and analysis system that mines the events recorded by the logging system installed on each of the CIS in order to detect events that affects CIS security. The log correlation and analysis system is installed and operated by the operator (or the service provider appointed to that effect) via a dedicated information system used only to detect events that are likely to affect the security of information systems.

3.2 Computer Security Incident Management

Information system security incident response

The operator creates and keeps up-to-date and implements a procedure for handling, response to and analysis of incidents that affect the functioning or the security of its CIS, in accordance with its ISSP.

The operator puts in place a dedicated information system to handle incidents, in order inter alia to store the technical records of incident analysis. The operator segregates the system from the CIS affected by the incident and stores the related technical records for a period of at least half-a-year. The operator takes into account, when designing the system, the confidentiality level of stored documents.

Incident Report

The operator creates and keeps up-to-date and implements procedures for incidents 'reporting.

Communication with competent authorities and CSIRTs

The operator implements a service that enables it to take note, without undue delay, of information sent out by its national competent authority concerning incidents, vulnerabilities, threats and relevant mappings (up-to-date inventory of CIS, interconnections of CIS with third-party networks, etc.). It implements a procedure for handling the information received, and, where appropriate, for taking the security measures required to protect its CIS. The operator provides its national competent authority with up to date contact details (department name, telephone number, and e-mail address) for this service. The operator is encouraged to connect its incident management with relevant Computer Security Incident Response Teams (CSIRTs).

PART 4 - RESILIENCE

3.1 Continuity of operations

Business continuity management

In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding business continuity management, in case of IT security incident.

Disaster recovery management

In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding disaster recovery management, in case of severe IT security incident.

3.2 Crisis management

Crisis management organization

The operator defines in its ISSP the organization for crisis management in case of IT security incidents and the continuity of organization's activities.

Crisis management process

The operator defines in its ISSP the processes for crisis management which the crisis management organization will implement in case of IT security incidents and the continuity of an organization's activities.

(…)

1.11 Identification of Operators of Essential Services: Reference document on modalities of the consultation process in cases with cross-border impact (CG Publication 07/2018)

Introduction

Where an operator provides services in more than one Member States, Article 5(4) requires that those Member States shall engage in consultation with each other before those Member States take a decision on the identification of OES. The purpose of this consultation is to facilitate the assessment of the critical nature of the operator, by the involved Member States, in terms of cross-border impact.

The cross-border consultation is a complex process, which involves the collection and exchange of ad-hoc and confidential information between the involved MS. With a view to streamline the consultation, this guide proposes two things:

a) A five step process which allows the involved Members States to engage in a dialogue with each other in order to fulfil the requirement of article 5(4); and

b) A list of data fields as a means to facilitate the information exchange during the consultation process. On the basis of this guideline the Member States can go beyond that proposed for exchange of information.

As regards the collection and exchange of ad hoc and confidential information between involved Member States, please note that such exchange should be subject to the following:

- the silence (acceptance) procedure i.e. a defined period of time after which if no comment is received, consultation is deemed to have taken place,

- should take place on a best effort basis from both Originating Member State (OMS) and Affected Member State (AMS) Single Point of Contact (SPOC); and

- should respect the need-to-know principle in order to avoid unnecessary sharing of information amongst different national SPOC (...)

1.12 Cross-border Dependencies: Guidelines for the Member States on voluntary information exchange on cross-border dependencies (CG Publication 01/2019)

Objective

The aim of these guidelines is to help Member States gather information on and map their cross-border dependencies and risks related to those dependencies which can eventually help them in applying nationally any risk mitigation measures deemed appropriate. They do not apply to information exchanges on such dependencies covered by the non-binding reference document on modalities of the consultation process in cases with cross-border impact as laid down in Article 5(4) to facilitate the assessment of the critical nature of operators of essential services (...)

1.13 Reference document on Incident Notification for Operators of Essential Services: Circumstances of notification (CG Publication 02/2018)

Purpose

Recognizing the solid and growing risk posed to OES and their potential impact on EU's economy and society and taking into account that some OES may be established in different EU Member States, the Group agreed that all may benefit from coherent approaches to the transposition of the NIS Directive with regard to incident notification for OES.

The Group also considered the need for Member States to be provided concrete and immediately usable recommendations to support their transposition process, instead of favouring an inclusive expert approach, which would have taken an excessive amount of time and would likely not have been produced before the deadline for the NIS Directive transposition.

As a consequence, as indicated in Article 14(7) of the NIS Directive, the Work Stream aimed at offering indications on how Member States may today address the transposition of article 14 (3) and (4) of the NIS Directive related to incident notification for OES. It has to be noted that this is a living document and it will continue to be updated and improved based on the state of the art threat landscape and the decisions taken by the Group.

(...)

Conclusions

The current study has uncovered some concerns that must be addressed while implementing the OES incident reporting provisions of the NISD. The multitude of sectoral approaches mirrored the numerous discrepancies between types of OESs and the corresponding business models adopted, thus creating a deep pool of sometimes incompatible variables that must be taken into account

when approaching such a regulation. For example, a simple parameter imposed by the Directive, such as "number of users", can mean different things to different types of providers, from simple clients of an electricity provider to potential patients of a hospital.

Achieving convergence between the myriad of existing approaches while sticking to the formal requirements might be troublesome. Nevertheless, the EU's first OES incident notification requirements as part of the first EU wide set of rules on cyber-security are a major step forward towards achieving a common level of resilience across the Union. In a perpetually fluctuating technological landscape that affects our livelihoods while having increasing economic and societal impact as a whole, a first step, in understanding the real threats and vulnerabilities that we have to confront, has been taken through the adoption of the NISD along with its two main requirements: mandatory incident notification and minimum security measures. From now on, a "small steps" approach must be applied in implementing the Directive, that has to undergo periodic reviews and updates.

This document provides a preliminary guideline on how incident notification provisions for OES could be effectively implemented across EU. Based on valuable input from Member States and companies directly impacted by the Directive, this guideline arises from their good practices in matters such as identifying types of incidents, parameters and thresholds and results in an outline proposal that can support harmonized implementation across EU.

(…)

1.14 Guidelines on notification of Operators of Essential Services incidents: Formats and procedures (CG Publication 05/2018)

Introduction

This document provides non-binding technical guidance for national competent authorities and/or the CSIRTs on the mandatory notification requirements in the NIS directive (2016/1148) for OESs (Article 14), for the requirement to inform other Member States in case of cross-border impact (Article 14), for the annual summary reporting by single points of contact to the NIS Cooperation Group (Article 10), and for the voluntary notifications (Article 20).

(…)

1.15 Guidelines on notification of Digital Service Providers incidents: Formats and procedures (CG Publication 06/2018)

Introduction

This document provides non-binding technical guidance for national competent authorities on the mandatory notification requirements in the NIS directive (2016/1148) for DSPs (Article 16), as further specified in the subsequent implementing regulation C(2018)471, for the requirement by the Member State of main establishment (Article 18) to inform other Member States in case of cross-border impact (Article 16), and for the annual summary reporting by single points of contact to the NIS Cooperation Group (Article 10).

(…)

1.16 Cybersecurity Incident Taxonomy (CG Publication 04/2018)

Goal

The goal of this document is to offer a common taxonomy for large scale cybersecurity incidents, as mentioned in the Commission Recommendation of 13 September 2017, also known as the

blueprint. This taxonomy has been welcomed by the General Affairs Council in its conclusions on 'EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises'1.

This taxonomy is to be used for the purpose of incident response coordination activities at Union level carried out in the framework of the Integrated Political Crisis Response (IPCR) arrangements. The scope of this taxonomy is cybersecurity incidents in general, for the sake of completeness.

This taxonomy could be useful also for information sharing across borders, annual summary reporting under the NIS directive, and international collaboration and information sharing.

It is important to underline here that this taxonomy addresses only the 'naming 'of cybersecurity incidents, and it does not address the 'processes 'for example for notifying or escalating incidents. Moreover, this incident classification does not exclude the use of additional taxonomies, such as sectorial taxonomies, in case a more specific classification is needed.

(…)

1.17 Sectorial implementation of the NIS Directive in the Energy sector Report (CG Publication 03/2019)

Introduction

The energy infrastructure is arguably one of the most complex and, at the same time, critical infrastructures that other business sectors depend upon to deliver essential services. Because of this dependency, a potential disruption for a long period can trigger a cascade of effects in other sectors of society.

In this light, the objective of this document is to collect information from the Member States on energy sector specific NIS Directive requirements. This will allow for a more consistent approach to energy cybersecurity at EU level as well as the identification of cascading effects, which might have a serious impact on many business sectors of society and even in other Member States´ economy.

This document is an output of Work Stream 8 led by experts from Austria, supported by experts from ENISA and involving the European Commission. It presents an overview of the status of implementation of Article 5 for the energy sector, analyses key findings, challenges and sectorial specificities. The document provides good practices and examples of implementation of the main NIS Directive requirements – identification criteria, security measures and incident reporting requirements specific for the energy sector.

The information collected for this document is a result of a survey developed by ENISA, Austria and the European Commission. The members of the Cooperation Group have been invited to participate in this survey. Overall, fifteen Member States responded and provided valuable feedback.

(…)

ENISA Publications

1.18 Technical Guidelines for the implementation of minimum security measures for Digital Service Providers (December 2016)

Executive Summary

Online marketplaces, online search engines and cloud computing services are considered as Digital Service Providers (DSPs) in the context of the recently adopted Directive (EU) 2016/1148

of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, hereafter referred to as the Network and Information Security (NIS) Directive.

The NIS Directive aims to bring cybersecurity capabilities on the same level of development in all the EU Member States. Its purpose is to ensure that exchange of information and cooperation related to security amongst Member States are efficient, including at the cross-border level. With NIS becoming a requirement, the introduction of specific laws in this area across the European Union will have a significant impact to all industry sec- tors including those relating to DSP categories.

Many businesses in the Union rely on these DSPs for the provision of their services. Some digital services could be an important resource for their users, including Operators of Essential Services (OES), and as such users might not always have alternatives available. The security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which depend on it and could consequently have an impact on key economic and societal activities in the Union. Such digital services might there- fore be critical for the smooth functioning of businesses that depend on them, for the internal market and cross- border trade across the Union.

It is essential for all Member States to make sure that they have minimum capabilities to ensure a high level of NIS in their territory and to improve the functioning of the internal market. Commonly defined security measures can support harmonised security practices across EU Member States and potentially enhance the overall level of NIS in the EU.

Therefore, ENISA has issued this report to assist Member States and DSPs in providing a common approach regarding the security measures for DSPs. Although ENISA has already drafted a set of security objectives in the context of cloud security in 2014, this study goes further than that by broadening the scope of its work and by including security objectives for all three categories of digital service providers. This study lists 27 Security Objectives (SOs) for DSPs. In those 27 SOs, security measures that map to the NIS Directive requirements are also included.

This particular initiative has been achieved by examining current information and network security practices for the DSPs across the EU. It has brought light to some important findings that can add to existing security objectives and measures in information technology infrastructures in Europe. It is recommended that stakeholders and responsible parties analyse their information security needs in detail in order to evaluate and adapt each of the security objectives and measures according to their specific business requirements.

(…)

1.19 Incident notification for DSPs in the context of the NIS Directive: A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive (February 2017)

Executive Summary

The NIS Directive is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. By ratifying a definite number of obligations across the EU, the Directive will help ensure a consistent approach to cybersecurity "with a view to achieving a high common level of security of networks and information systems within the Union so as to improve the functioning of the internal market". The main points of the NIS Directive can be summarised as follows: improved cybersecurity capabilities at national level, increased EU-level cooperation,

security measures and incident reporting obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP). The scope of this study is limited to relevant provisions of the NIS Directive on Digital Service Providers (DSPs) and their current activities in this field.

According to one of the provisions of the NISD, Member States must ensure that DSPs notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service. In determining the "substantial impact", the Directive mentions just five indicators to be used without providing other details.

As the Directive provides only a sketchy description of the incident notification concepts and the overall process, the main goal of this document is to develop a set of guidelines for all concerned stakeholders (EU level authorities, public, private), aimed at supporting the implementation of the NIS Directive requirements regarding mandatory incident notification for Digital Service Providers.

A useful description of the roles and responsibilities of all stakeholders involved is provided. From DSPs to EU level bodies involved, each part plays an important role in securing EU's cyber future. National authorities are responsible for managing the process at their level, while the Cooperation Group is established as a body that will support and facilitate strategic cooperation and the exchange of information among Member States. The interaction between involved bodies becomes crucial as the information flow regarding incidents must be properly assured throughout EU.

Establishing a clear view of the incident notification process, is a must for a proper implementation. Such a view, compiled from all requirements of the Directive, is included in this document. Certain aspects such as the main EU establishment of an DSP, cross border cooperation, the public awareness about incidents, relationship with law-enforcement are all explained. For a better understanding, the possible place occupied by the mandatory incident notification process within the generic incident management practices is explained.

Knowing what incidents have to be reported is equally important in the reporting process. As the Directive provides only some theoretical concepts that must be followed when reporting incidents, the current guidelines give an exhaustive description of the incident types covered by the NISD.

Further on, clarifications on the parameters that must be used when notifying are also important in the reporting process. The notions provided by the Directive are supplemented with technical interpretations and tips on how to apply them. A simple notion as "number of users" can raise multiple issues when trying to apply it to search engines or cloud providers.

Although at first sight we might consider the incident reporting topic as straightforward and easy-going, the current study has uncovered serious issues that must be addressed while implementing the DSP incident reporting provisions of the NISD. The multitude of technical approaches mirrored the numerous discrepancies between types of DSPs and the corresponding business models adopted, thus creating a deep pool of sometimes incompatible variables that must be taken into account when approaching such a regulation. For example, a simple parameter imposed by the Directive, such as "number of users", can mean different things to different types of providers, from simple visitors or registered individuals to corporate users and dependant services.

EU's first DSP incident notification requirements as part of the first EU wide set of rules on cyber-security are a major step forward towards achieving a common level of cyber-security across the Union. In a perpetually fluctuating technological landscape that affects our livelihoods while having increasing economic and societal impact as a whole, a first step, in understanding the real threats and vulnerabilities that we have to confront, has been taken through the adoption of the NISD along with its two main requirements: mandatory incident notification and minimum

security measures. From now on, a "small steps" approach must be applied in implementing the Directive, that has to undergo periodic reviews and updates.

This document provides preliminary guidelines on how incident notification provisions for DSPs could be effectively implemented across the EU. Based on valuable input from Member States and companies directly impacted by the Directive, this guideline arises from their good practices in matters such as identifying types of incidents, parameters and thresholds. The overall result is an outline technical proposal that can tentatively be used in the implementation process.

At the same time, this guideline serves as a technical input to the foregoing process of adopting the implementing act that will further specify details regarding the incident notification provisions of the NISD.

(…)

1.20 Good practices on interdependencies between OES and DSPs (November 2018)

Executive Summary

The Network and Information Security (NIS) Directive entered into force in 2016, becoming the first piece of European legislation dealing with cybersecurity. The directive was created with the objective of boosting the overall level of cybersecurity in the European Union. It does so by increasing the cybersecurity capabilities in the Member States, by enhancing cooperation on cybersecurity among the Member States, and by requiring Operators of Essential Services (OES) and Digital Services Providers (DSPs) to manage their risks. In relation to the latter, an important element of the risk to be assessed is the one of the dependencies of the services offered on other services of either OES or DSPs. These dependencies might be of either national or cross-border nature.

A glance at the interdependency landscape reveals a number of emerging interdependencies between OES/DSPs at both system and service level. There is an increasing number of cybersecurity incidents that, due to these interdependencies, either propagated across organisations, often across borders, or had a cascading effect at the level of essential services.

In order for OES, DSPs and National Competent Authorities (NCAs) to effectively identify and assess interdependencies, a framework based on a 4-phase approach appears to be a suitable way forward. Existing methods, tools and good practices for interdependencies can easily be mapped to these 4 phases based on the respective individual or sectorial specificities and needs. The development of indicators for the interdependencies' assessment, which are mapped to well-known and widely used industry standards and frameworks would also constitute a practical approach.

This report includes a set of recommendations for OES, DSPs and NCAs to effectively address interdependencies in their risk assessments, including:

- OES and DSPs should conduct empirical investigations to collect data

- OES, DSPs and NCAs should develop and integrate methodologies and tools

- OES and DSPs should develop expertise via awareness and training

- NCAs should work towards developing a common taxonomy of incident impact assessment

- OES and DSPs should address interdependencies at operational level

- NCAs should facilitate information sharing.

(…)

1.21 Guidelines on assessing DSP and OES compliance to the NISD security requirements: Information Security Audit and Self-Assessment/ Management Frameworks (November 2018)

Executive Summary

According to the NIS Directive Articles 14, 15 and 16, one of the key objectives is to introduce appropriate security measures for operators of essential services (OES) as well as for the digital service providers (DSP) in an effort to achieve a baseline, common level of information security within the European Union (EU) network and information systems. Information security (IS) audits and self–assessment/ management exercises are the two major enablers to achieve this objective.

This report presents the steps of an information security audit process for the OES compliance, as well as of a self-assessment/management framework for the DSP security against the security requirements set by the NIS Directive. In addition, it provides an analysis of the most relevant information security standards and frameworks to support OES and DSP in practicing the above exercises in the most tailored and efficient manner.

The report identifies numerous parameters towards the successful conduct of information security audits as well as self-assessment/management. Specifically it:

- Proposes an information security audit methodology that could be utilized to facilitate the audit process for OES by the NCA and DSP security self-assessments e [*sic.*];

- Provides an indicative guideline (set of questions) accompanied by evidence that could be utilized to facilitate the overall audit process;

- Proposes to DSP an indicative list of questions, together with relevant evidence, that could facilitate their self assessment exercises against the security requirements prescribed in article 16(1) of the NIS Directive;

- Presents post-audit actions for the NCA with a view to extract benefit and/or knowledge, following an information security audit exercise;

- Illustrates all the information security lifecycle phases and highlights key issues in each phase (e.g. scoping and main challenges during the pre-audit/ planning phase); and

- Presents a comparison of IS audit and self-assessment/management frameworks and methodologies and their correlation with relevant IS audit standards.

Overall, this report is a guidance to national competent authorities in supporting the implementation of the requirements stemming from article 14, 15 and 16 of the Directive.

(…)

1.22 Gaps in NIS standardisation: Recommendations for improving NIS in EU standardisation policy (November 2016)

Executive Summary

This report recommends that the European Commission, with the support of the Member States, pursuant to the NIS Directive, adopt a standards based framework for the exchange of threat and defensive measure information that impacts the functioning of Network Information Infrastructure (NII). The capabilities from this framework underscore NII as Critical Infrastructure of the EU and its Member States.

This report recognizes the work already addressed by a number of European bodies including the designated European Standardization Organisations (CEN, CENELEC and ETSI) and the Cyber Security Focus Group (CSCG), the European Reference Network for Critical Infrastructure Protection (ERNCIP), and individual Member States who have already taken steps to facilitate information sharing between Computer Security Incident Response Teams (CSIRTs). The recommendations of this report include extending the technical basis for information sharing in the following ways:

- Adopting open standards in threat exchange based on the globally accepted STIX/TAXII/CyBOX platform to be prepared as an European Norm (EN) defining the syntax and semantics of the data and the necessary transfer protocol, and an accompanying guide to the implementation of the standard

- Extending the risk analysis and defensive measures capabilities defined in current standards to allow Member States to address the NII and NIS provisions necessary to mitigate risk both at national and regional level. This should be prepared as an EN extending the capabilities already described in ETSI TS 102 165-1, ETSI TR 103 305, ISO/IEC 15408 and in relevant ISO/IEC JTC1 2700x series standards.

In making the recommendations above, it is noted that it is not possible to separate provisions for NIS from general provisions for cyber security which have been developed by a broad array of ICT standards bodies and implemented to varying extents by the entities subject to the NIS Directive. A significant concern consists in the fact that EU Regulation No 1025/2012 referenced by the NIS Directive only defines a small handful of organisations as constituting standardization bodies. This is not an accurate reflection of the current state of the market, nor those used within the highly specialized sectors to which the Directive applies.

Furthermore, NII, NIS and Cyber security cannot be geographically isolated and applied only to the European Union. This distributed complexity should be considered in implementing of the necessary information sharing required for effective NIS. Thus many of the capabilities of the NII, of commercial necessity, will be implemented using software and hardware from a global market and not a market restricted to the EU.

(…)

1.23 Improving recognition of ICT security standards: Recommendations for the Member States for the conformance to NIS Directive (December 2017)

Executive Summary

This report is a continuation and an extension of previously carried out ENISA work on approaches to the NIS Directive by Member States, which have provided recommendations on standardisation and have outlined the use and management of CSIRTs.

This document provides the results of an assessment of the maturity of the implementation of the European Cyber Security Standardisation activities in the EU Member States with respect to the NIS Directive concerning measures for a high common level of security of network and information systems across the Union. The main assertions this report makes include the following:

- Standardisation for compliance with the NIS Directive is essential;

- Recognition of standardisation in policy is low;

- Utilisation of standards give value to Member States and their infrastructure;

- Utilisation of standards raises Cyber Security levels;

- Utilisation of standards provides sustainability and interoperability at European level.

The current market research has clearly shown that the information security/cyber security standard development ecosystem is healthy and fast moving. Few gaps actually exist and to implement the NIS Directive choosing the rights ones and implementing them is of paramount importance.

In the scope of this survey a questionnaire was sent to the Member States representatives and used as the basis of data gathering either in the form of interviews, or by directly completing it and sending responses to the authors. A summary of the responses given have been collated and summarised.

The content of these responses does not allow to identify whether Member States perceive the existence of a gap in current available standardisation. However, the content, and general limitations in the cohesion amongst Member States suggests that there is insufficient guidance from the specialists in the field (e.g. national normalization institutes, European institutions etc.), on which of the many standards available are to be used. It is reasonably straightforward and it follows on the current rate on transposition, to suggest that all Member States are aware of the NIS Directive and their responsibilities in implementing it. What is less clear is the role that standards have in the NIS Directive implementation.

There is insufficient information with regard to the responses to conclude that a lack of knowledge of standards exists. This suggests however that if an appropriate standard is available, it will be adopted. For example, even though the ISO27000 series of standards are in the form of broad guidance, there is a well-established eco-system that addresses their implementation.

A major concern is that the NIS Directive domain, and compliance with the NIS Directive requirements, is often perceived as a purely national prerogative. Where international, cross-border, information sharing is required, this has been perceived as in the domain of existing CSIRT relationships used for reporting security incidents and not directly as an element of NIS Directive compliance.

At the operational level there is very little specified for standards-based NIS Directive compliance and this is one area where ETSI, for example, has made some contributions. However, there are no mandates at either national or European level to guide this activity at the implementation level.

In light of the above, the following solutions are recommended to mitigate the lack of overall awareness and trainings [*sic*.] on the role of standards in NIS Directive compliance and to encourage wide deployment of common security platforms in the OES and PDS entities:

- Training initiatives by the European Commission and ENISA through workshops for Member States 'relevant agencies

- Promotion of new work items in the European SDOs for some areas (e.g. criteria for defining OES / DSP) or the adoption of appropriate standards in Europe where existing (for example information exchange, where several mature efforts already are in place, like STIX)

- Repeat the information gathering as performed within the elaboration of this study after an adequate interval of time

(…)

1.24 Mapping of OES Security Requirements to Specific Sectors (December 2017)

Executive Summary

According to the Directive (EU) 2016/1148 issued by the European Parliament and the Council, hereafter referred to as 'Network and Information Security (NIS) Directive', specific types of

entities which provide essential services to the European internal market, shall be identified by the Member States. The business sectors for these entities are depicted in Annex II of the NIS Directive.

One of the main objectives of the NIS Directive is to enact security measures for operators of essential services (OES) across the European Union, in order to achieve a high common level of Security of Network and Information Systems.

The current report provides a substantial and comprehensive mapping of the security requirements for OES, as they have been agreed in the NISD Cooperation Group, to sector specific information security standards. Initially, ENISA conducted desktop research on international security standards, guidelines and good practices per sector. Finally, the security requirements for OES were mapped to international standards used by operators covering all business sectors under scope. This report is a living document that we will augment on a regular basis to keep it up to date with the latest developments.

(…)

1.25 Stock taking of information security training needs in critical sectors (December 2017)

Executive Summary

The European Union's Directive on security of network and information systems (NIS Directive) asserts that "network and information systems and services play a vital role in society", and that the "magnitude, frequency and impact of security incidents are increasing, and represent a major threat". Given that urgency, the NIS Directive goes on to argue that "operators of essential services" need to identify "which services have to be considered as essential for the maintenance of critical societal and economic activities". This is in fact referring to the operators in the so-called critical sectors, with those being: energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure.

The protection of these seven critical sectors should have the highest priority, because when they are under threat, the functioning of society itself and the well-being of its citizens are at stake. As part of this effort, it is extremely important to increase the competences of cyber security personnel. This requires the availability of high quality trainings [*sic.*] across the board, available to all critical sectors.

Within the critical sectors, there are significant differences regarding the maturity level of cyber security. Therefore, some of the critical infrastructure operators will not be as ready as others, to counter the risks resulting from new cyber security threats in a timely and adequate manner.

With the emphasis that the NIS Directive places on the importance of the seven critical sectors, this study aims to identify the current situation in these sectors in regard to the available cyber security trainings [*sic.*] , and if there are any training needs specific to each of the sectors, beyond the generic needs for such trainings.

Over the past years, ENISA has developed a wide range of cyber security trainings [*sic.*], and also delivered the training content to several national and governmental CSIRTs (Computer Security Incident Response Teams) as well as their constituents. The next important question that this study set out to answer is if and how the ENISA training portfolio actually is useful for the seven critical sectors – and what could be done to improve the suitability of that portfolio to the existing training needs.

The main general conclusions are:

- the cyber security training field is extensive and diversified, but does not sufficiently address the issue of raising the cyber security resilience of critical infrastructure: CIP-related trainings are still a niche

- there is a shortage of specialised trainings in the field of ICS/SCADA systems cyber security – which is an essential element in countering operational threats (e.g. in the energy sector)

- there are very few trainings specialising in the specific threats encountered in the different (sub)sectors

- cyber security awareness raising trainings are lagging behind

- there is a shortage of trainings [*sic.*] in regard to decision making as a result of data leakages or privacy incidents

- there is a pressing need for trainings [*sic.*] related to GDPR, since this will affect every sector, and could have an operational impact on the organization.

As for the fit of ENISA's current training offer to the needs of the seven critical sectors, the study has found that:

- ENISA should present the context of threats and risks related to each sector in the trainings. In particular, dependencies and mutual influence of infrastructures operating in different sectors should be explained, and their possible impact on cyber-security issues concerning e.g. global payments or air traffic control

- ENISA should provide trainings in more local languages

- ENISA should determine whether cyber ranges and gamification based trainings will likely provide a more effective approach than traditional trainings [*sic.*]. On-demand training accessibility is gaining in importance.

- ENISA is advised to organise a pilot study in for instance the transport sector to further gauge the results of this study and come to implementable proposals on how to improve the training situation in that sector. This approach may be used for other sectors too.

(…)

1.26 Good practice guide for CERTs in the area of Industrial Control Systems: Computer Emergency Response Capabilities considerations for ICS (October 2013)

Executive summary

Industrial Control Systems (ICS) are indispensable for a number of industrial processes, including energy distribution, water treatment, transportation, chemical, government, defence and food processes. Though until a few decades ago ICS functioned in discrete environments, nowadays they tend to be connected to the Internet. This enables streamlining and automation of industrial processes, but carries with it the risk of exposure to cyber-attacks. The ICS are lucrative targets for intruders like criminal groups, foreign intelligence, phishers, spammers or terrorists. Therefore, the ability to respond to and mitigate the impact of ICS incidents is crucial for protecting critical information infrastructure and enhancing cyber-security on a national, European and global level.

This document is an initial attempt to provide a good practice guide for the entities that have been tasked to provide ICS Computer Emergency Response Capabilities (ICS-CERC). On the other hand, this guide does not have the ambition to prescribe to the EU Member States which entities should be entrusted with provision of ICS-CERC services.

This document builds upon the current practice of CERTs with responsibilities for ICS networks, and also on the earlier work of ENISA on a baseline capabilities scheme for national/ governmental (n/g) CERTs. Consequently, it employs a similar approach in addressing the topics relevant for ICS-CERC provision, by using four categories of baseline capabilities: mandate, service portfolio and operations in relation to ICS-CERC and, last but not least, cooperation with the other ICS stakeholders. These four categories of capabilities are mutually interdependent.

In the chapter on mandate capabilities the guide delves into formal processes for the establishment of ICS-CERC. It mentions factors that need to be taken into account when building ICS-CERC rather than building response capabilities for 'ordinary 'ICT systems. The guide also addresses the advantages and disadvantages of concrete types of the mandate: ICS sector-specific, national, regional and global. It defines the constituencies for ICS-CERC and offers a variety of international sources of inspiration for the mandate and other formal aspects of ICS-CERC.

Operational capabilities (technical) focus on actual ICS-CERC services to be provided, especially in the main phases of the incident management cycle. The guide also briefly touches upon the question of how to maintain, develop and improve ICS-CERC once it has been established.

The chapter on operational capabilities (organisational) deals with operational aspects required for the provision of ICS-CERC services and also with dedicated personnel and their qualifications. The guide highlights the importance of training and further education for the staff responsible for ICS-CERC and also raises the topic of a suitable hosting organisation for ICS-CERC.

The chapter on co-operational capabilities summarises the main reasons for on-going cooperation between CERTs providing ICS-CERC services and other ICS stakeholders. In this context, the peculiarities of both national cooperation (with ICS providers, vendors or CERTs in the country) and cross-border cooperation (international initiatives in the area of ICS protection like CIGRE, ESCoRTS, IEEE and others) are discussed.

Wherever appropriate, examples of current practices related to handling ICS incidents are presented. However, it should be noted that established CERTs in Europe still have very limited experience in and contact with ICS-CERC services. For these reasons, this guide needs to be considered a living document, which will need to be updated in accordance with wider deployment of ICS-CERC in Europe. ENISA is ready to provide support to the teams responsible for the provision of ICS-CERC services. It already provides online training material for the CERTs relating to attacks on critical information infrastructure (scenario 13 of CERT training material).

(…)

1.27 CSIRT Capabilities: How to assess maturity? Guidelines for national and governmental CSIRTs (December 2015)

National and governmental CSIRTs are essential for every country that is concerned about protecting its digital assets, starting from sensitive government information to its citizens and their information. The CSIRTs 'role is very wide, from security incident response and management to various sophisticated technical services and awareness-raising and educational activities. When dealing with cyber incidents, CSIRTs have to work closely with law enforcement and other authorities, but no other authority in the cyber ecosystem is in the better position to help users and institutions to stop cyber incidents, to understand why they could happen and what to do to prevent them from happening again; this is the unique role of a CSIRT.

Currently in the EU, governmental CSIRTs are typically used to protect the cyberspace of governmental institutions including critical infrastructure as well as to ensure cyber-crisis management. National CSIRTs, on the other hand, are playing different roles in different countries. In some countries they are responsible for the whole IP address space of that country, in others they also take the role of 'last resort 'when no security contact point for an IP address can be

found. In any case, when another country has to be contacted regarding solving an incident, national CSIRTs are often asked to help to find the right contact person. Increasingly CSIRTs expect other teams with comparable competences to react to their requests in a timely manner and to handle shared information professionally. A maturity process and certification can help to ensure that these expectations are met. A high level of maturity (certification or similar activities) is also desirable for successful participation in CSIRT cooperation networks working in Europe. Many governmental and national CSIRTs are also responsible for crisis management and critical infrastructure protection processes in their countries. Considering the importance and complexity of these processes, the responsible team's maturity is one of the key factors determining success or failure.

This document focuses on the maturity of national and governmental Computer Security and Incident Response Teams (CSIRTs) and the Trusted Introducer1 certification scheme for CSIRTs as an indicator of the maturity level of teams. The issues covered are described from two points of view: the perspective of the team that is preparing for the certification process on the one hand and of teams that have already undergone certification and even recertification on the other. The aim of this document is to be a guiding tool for those national and governmental CSIRTs which are considering reaching the next level of maturity and good understanding of their capabilities.

This document gives recommendations for CSIRTs on how to improve and mature and be better prepared to protect their constituencies.

ENISA has carried out a considerable amount of work in this area, and this document contributes by sharping the role of ENISA in helping national and governmental CSIRTs on their way to a higher maturity level (…)

1.28 Strategies for Incident Response and Cyber Crisis Cooperation (August 2016

Executive Summary

This document was prepared for the NIS Platform WG2 members introducing the main functions of CSIRTs from incident handling to crisis coordination – a high-level summary of the basics of incident response based on ENISA's previous work on CSIRTs and resilient European infrastructures. The current version of this document is an updated version of the one published in March 2016.

The Network and Information Security (NIS) Platform was created in 2013 to help European stakeholders carry out appropriate risk management, establish good cyber security policies and processes and further adopt standards and solutions that will improve the ability to create safer market conditions for the EU. All this was brought to life as a contribution to the implementation of the Cyber Security Strategy of the EU.

This document is an input for the NIS Platform for the discussion on incident response and cyber crisis coordination.

The document focuses on incident response: it briefly introduces what incident response is, who the main actors are, what baseline capabilities these entities should possess in order to effectively combat cyber-attacks, and what challenges there may be that impede efficiency in incident response. The notion of Computer Security Incident Response Teams (CSIRTs) as key players in incident response is introduced. Descriptions of incident response mechanisms will be elaborated, taking into account national-level cyber security strategies, cyber crisis coordination and management covering both escalation and communication between CSIRTs and government bodies.

The core material of the document was developed based on previous work undertaken by ENISA in the field of CSIRTs and Critical Information Infrastructure Protection (CIIP) and resilience. The main topics used as input for this document cover the following:

- findings and recommendations published under the baseline capabilities of CSIRTs and a brief description of incident response mechanisms;

- work done in the field of national cyber security strategies with special regard to implementation and evaluation of these strategies;

- aspects of cyber crisis cooperation and management focusing on escalation mechanisms and ways of further enhancing crisis cooperation mechanisms, such as mutual aid, training and exercising and Standard Operating Procedures (SOPs).

Some challenges will be raised on the typical issues that slow the incident response mechanisms, and to address these challenges, ways of enhancing incident handling cooperation will be provided.

(…)

1.29 A good practice guide of using taxonomies in incident prevention and detection (December 2016)

The aim of this document is to provide good practices on using taxonomies for incident detection and prevention by taking into account the input received from the CSIRT community and relevant information from previous ENISA studies. In addition, it provides conclusions and recommendations on improvements that can be made on current taxonomies.

(…)

1.30 ENISA Maturity Evaluation Methodology for CSIRTs (April 2019)

Executive Summary

The primary target audience for this report is the EU CSIRTs network teams, and their leadership. However it needs to be stressed here that this report, and especially the maturity self-assessment that it contains, will be of use to all types of CSIRTs all over the world.

The EU Network and Information Security Directive (NIS Directive) creates a CSIRTs network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". The Directive states that each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I (requirements), covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well–defined process. The Directive gives high-level requirements that designated CSIRTs must observe, and tasks that they must perform.

In order to provide input to the designated CSIRTs on this topic, ENISA performed a continuation of the 2016 study on CSIRT maturity, focused on the national teams expected to join the CSIRTs network. To recapitulate, the 2016 study had the following main results:

1. A sustainable and implementable approach towards assessing and improving maturity is best based on a measurable set of quantities, or parameters. The SIM3 model as is commonly used in Europe serves as an excellent basis for this, with some additions based on especially the NIS Directive requirements.

2. The three-tier approach towards maturity that ENISA adopted in the 2013 report "CERT community - Recognition mechanisms and schemes" can be used to define a scale of three steps

when adopting the SIM3 maturity model to assess CSIRT maturity: basic, intermediate and advanced.

3. A proposed specific definition of those three steps for the benefit of the CSIRTs network, coupled with the suggestion to define a validation process based on self-assessments and peer-assessments.

By adopting the approach proposed in the 2016 study, the CSIRTs network would have immediate access to a clearly laid out CSIRT maturity improvement process, that is not only implementable and sustainable, but also based on a proven best practice: the SIM3 model is in use in the European TF-CSIRT Trusted Introducer community since 2009, for self-assessments but also for over 20 certifications so far, including 7 members of the CSIRTs network. The Global Forum on Cyber Expertise (GFCE3) has adopted SIM3 as their CSIRT maturity framework in 2015.4 In Japan, the Nippon CSIRT Association (NCA5), with well over 200 member teams, is basing their maturity improvement scheme on SIM3.

A growth path was suggested that reaches the basic step within one year, intermediate two years later and advanced another two years later: a total of five years 'maximum which is in line with the CSIRTs network work roadmap. Achieving the basic step would already allow a minimum of successful co-operation between teams on incident handling, the higher steps are needed to allow the members of the CSIRTs network to interact on all steps, including pro-actively, thus truly giving meaning to the word CSIRTs network.

(…)

See also: ENISA CSIRT maturity assessment model (April 2019)

1.31 EU MS Incident Response Development Status Report (November 2019

Executive Summary

Following the recent transposition of the NIS Directive (NISD) into European Member States (MS) legislation, this study aims to analyse the current operational Incident Response set-up within NISD sectors and identify the recent changes. The study provides a deeper insight into NISD sectoral Incident Response capabilities, procedures, processes and tools to identify the trends and possible gaps and overlaps.

Incident Response Capabilities (IRC) within NISD sectors is a growing concern to tackle potential incidents which could have a major impact on European societies and citizens. To assess IRC, the analysis framework for the research included the following aspects:

- Impact of the NIS Directive on national CSIRT/IR layout and operational set-up in the NISD sectors;

- IR cooperation and operational models within the NISD sectors

- IRC development in the NISD sectors

- Lessons learned and recommendations.

A series of seven findings were identified while conducting the research activities.

Key Finding #1 – Member States 'organisational culture and resources tend to shape the overall IR layout and set-up

Depending on whether a Member State's organisational culture is centralised or decentralised, the Incident Response layout and set-up is often structured in a similar manner, i.e. with a central authority or instead with shared responsibilities between different actors. The main entities in

charge of Incident Response at national level, tend to be the national CSIRT and the Operator of essential Services (OES. However, the mandate and the resources of the National CSIRT or national cybersecurity authority is another important element influencing a centralised or distributed incident response model.

Key Finding #2 – The Directive's main positive impact was to clarify actors 'roles and responsibilities within the IR organisation

The main positive impact of the Directive was to improve the IR organisation and governance by clarifying actors 'roles and responsibilities. The data collected also suggest that the NISD had an unequal effect from one country to another. Indeed, this positive impact is less visible in Member States with a more mature layout and pre-existing national regulations to govern incident response in NISD sectors. However, the Directive has led/is leading to the formal identification of OES in countries who had not previously done so.

Key Finding #3 – The implementation of the NISD raises operational and regulatory challenges for the MS regulators and competent authorities

The implementation of the Directive raises operational and regulatory challenges, in particular for the definition of OES and competent authorities and the legal balance between sharing information and respecting privacy regulations. The operational implementation of the Directive in the Member States also highlights MS willingness to move forward since most of them extended the number of sectors targeted and their scope.

Key Finding #4 – The success of demand or regulatory drivers for the creation of sectoral IR entities and capabilities depends on IR layout maturity

The creation of sectoral IR entities and capabilities is driven by both operational demand and policy regulation. A blend of bottom-up and top-down incentives could be the most efficient driver to enhance capabilities, however an important element to take into account is the MS IR layout maturity. In countries with a very mature or centralised IR layout, there is less need for sectoral IRC. For all NISD sectors and/or sub-sectors, the main entities in charge of IR for 51% of the respondents are the national CSIRT and the OES

Key Finding #5 – Sectoral CSIRTs rely on similar notification and reporting tools as National CSIRTs but provide sector-specific knowledge and expertise to their constituents

Both national CSIRTs and sectoral CSIRTs have developed mature reporting processes and notification tools. The main added value of sectoral CSIRTs is to provide services specific to their sectors 'needs, in particular a more in-depth knowledge of the threat and actor landscape, better adapted tools and solutions and operational expertise. Sector-specific regulations which include guidelines and requirements for reporting and management of incidents are crucial to enhance capabilities at the sectoral level. However, there is a lack of skilled staff, making it difficult for sectoral CSIRTs to reach full capacity.

Key Finding #6 – There is a growing number of sectoral cooperation and information- exchange initiatives, yet they often lack visibility or resources to sustain their efficiency

There is a multiplication of information exchange tools and initiatives to facilitate cooperation at sectoral, national, regional and EU level. These initiatives can take various forms and be more or less formalised. This quantitative evolution is an encouraging sign but does not provide information on the quality and outcomes of the exchanges. The long-term benefits of these initiatives will depend on the presence of both organisational and structural elements to sustain the efficiency of the initiatives.

Key Finding #7 – Training at sectoral level is key to foster and enhance preparedness

Training is an area of constantly growing interest for sectoral CSIRTs and for other operational entities and it is considered as a crucial pillar of the cybersecurity value chain and IR actors ' preparedness and expertise. Interesting good practices to organise training have been gathered by national CSIRTs, which could provide an answer to the need for skilled personnel training opportunities.

Recommendations to ENISA
- Knowledge: Collect deeper insights on both national and sectoral CSIRT maturity when the NISD will have been fully practically implemented;

- Cooperation: Bolster cross sectoral knowledge between the stakeholders;

- Information sharing: Continue to collect available resources to enhance IRC & enhance information-sharing and build a repository;

- Training: Evaluate a possibility to develop a continuum for training activities which include assessing sectors trainings needs, promoting the ‘‘train-the-trainers» approach and developing basic sectoral trainings.

Recommendations to the IRC community (National and sectoral CSIRTs

- Transparency: Publish a clear list of the sectors covered within NISD at national level (same as the NISD or extended);

- Information sharing: Encourage the use of secure communication tools, common taxonomy and sharing of lessons learned after incident with peers and everywhere; The responsible disclosure of vulnerabilities should be fostered by setting incentives;

- Cooperation: Build trust within communities and engage with OES and DSP;

- Resources: the IR community should have adequate resources to conduct their missions.

(…)

1.32 European Commission Press Release 30 October 2020: Cybersecurity: Commission urges Belgium, Hungary and Romania to comply with their obligations regarding operators of essential services

The Commission decided today to send reasoned opinions to Belgium, Hungary and Romania regarding their failure to notify the Commission with information related to the identification of operators of essential services. The Commission, as set out in the Directive on security of network and information systems (NIS Directive (EU) 2016/1148) required this information to assess the consistency of approaches different Member States take when identifying operators of essential services. The deadline to submit the information was by 9 November 2018.

Today's reasoned opinions follow the letters of formal notice sent by the Commission in July 2019 to all three countries. In the case of Belgium, the missing information includes the number of operators in several critical sectors such as energy, transport, health and drinking water supply and distribution, as well as information about existing thresholds to identify them (used in the identification process). Hungary needs to notify about the operators of essential services for the transport sector that are still missing, while Romania's authorities still need to notify about national measures allowing for the identification of operators, the number of operators of essential services and thresholds used in the identification process. Belgium, Hungary and Romania now have two months to take the necessary measures to comply; otherwise, the case may be referred to the Court of Justice of the EU.

4. Sector-specific requirements: the electricity sector

Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (notified under document C(2019) 2400)

(…)

Whereas:

(1) The European energy sector is undergoing an important change towards a decarbonised economy, while ensuring security of supply and competitiveness. As part of that energy transition and the related decentralisation of power generation from renewable sources, technological progress, sector coupling, and digitalisation are turning Europe's power grid into a 'smart grid'. At the same time, this also brings new risks as digitalisation increasingly exposes the energy system to cyberattacks and incidents which may jeopardize the security of energy supply.

(2) The adoption of all eight legislative proposals of the 'Clean Energy for all Europeans 'Package including the Energy Union Governance as stepping stone, allows to create a favourable environment for the digital transformation of the energy sector. It also acknowledges the importance of cybersecurity in the energy sector. In particular, the recast of the Regulation on the Internal Market for Electricity provides for the adoption of technical rules for electricity such as a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management. The Regulation on Electricity Risk Preparedness broadly follows the approach chosen in the Regulation on Security of Gas Supply; stressing the need to properly assess all risks, including those related to cybersecurity, and proposing to adopt measures to prevent and mitigate those identified risks.

(3) When the Commission adopted the EU Cybersecurity Strategy in 2013, it identified strengthening the Union's cyber-resilience as a priority. One of the key deliverables of the Strategy is the Directive on Security of Network and Information Systems (hereafter, the 'NIS Directive'), which was adopted in July 2016. As the first piece of horizontal EU legislation on cybersecurity, the NIS Directive boosts the overall level of cybersecurity in the Union through the development of national cybersecurity capabilities, the increase of EU-level cooperation and the introduction of security and incident reporting obligations for companies referred to as 'operators of essential services'. Incident reporting is mandatory in key sectors, including the energy sector.

(4) When implementing preparedness measures in cybersecurity, the relevant stakeholders, including operators of essential services in energy as identified under the NIS Directive, should take into account the horizontal guidance issued by the NIS Cooperation Group established under Article 11 of the NIS Directive. That Cooperation Group, which is composed of representatives of Member States, the European Agency for Cybersecurity (ENISA) and the Commission, has adopted guidance documents concerning security measures and incident notification. In June 2018, that Group created a dedicated work stream on energy.

(5) The 2017 Joint Communication on Cybersecurity acknowledges the importance of sector specific considerations and requirements at EU level, including in the energy sector. Cybersecurity and possible policy implications have been the subject of a comprehensive discussion process in the Union over the recent years. Consequently, there is rising awareness today that individual economic sectors face specific cybersecurity issues and, therefore, need to develop their own sectoral approaches in the wider context of general cybersecurity strategies.

(6) Information sharing and trust are key elements in cybersecurity. The Commission aims to increase the sharing of information among the relevant stakeholders by organising dedicated events, as for examples, the high-level roundtable on cybersecurity in energy organised in Rome in March 2017 and the high-level conference on cybersecurity in energy organised in Brussels in

October 2018. The Commission also wants to enhance the cooperation between relevant stakeholders and specialised entities such as the European Energy Information Sharing and Analysis Centre.

(7) The Regulation on ENISA, the 'EU Cybersecurity Agency', and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act Regulation') will strengthen the mandate of the EU Agency for Cybersecurity so as to better support Member States in tackling cybersecurity threats and attacks. It also creates a European cybersecurity framework for the certification of products, processes and services that will be valid throughout the Union and is of particular interest for the energy sector.

(8) The Commission has put forward a Recommendation addressing cybersecurity risks in the 5th generation (5G) of network technologies by setting out guidance on appropriate risk analysis and management measures at national level, on developing a coordinated European risk analysis and on establishing a process to develop a common toolbox of best risk management measures. Once rolled out, 5G networks will form the backbone for a wide range of services essential for the functioning of the internal market and operation of vital societal and economic functions such as energy.

(9) This Recommendation should provide non-exhaustive guidance to Member States and relevant stakeholders, in particular network operators and technology suppliers, for achieving a higher level of cybersecurity in view of the specific real-time requirements identified for the energy sector, cascading effects and the combination of legacy and state-of-the-art technologies. This guidance aims at helping stakeholders keep in mind the specific requirements of the energy sector when implementing internationally recognised cybersecurity standards.

(10) The Commission intends to regularly review this Recommendation based on the progress made across the Union in consultation with Member States and relevant stakeholders. The Commission will continue its efforts to strengthen cybersecurity in the energy sector, notably through the NIS Cooperation Group, which ensures strategic cooperation and exchange of information among Member States in cybersecurity,

(…)

SUBJECT MATTER

(1) This Recommendation sets out the main issues related to cybersecurity in the energy sector, namely real-time requirements, cascading effects and combination of legacy and state-of-the-art technology, and identifies the main actions for implementing relevant cybersecurity preparedness measures in the energy sector.

(2) In applying this Recommendation, Member States should encourage the relevant stakeholders to build up knowledge and skills related to cybersecurity in the energy sector. Where appropriate, Member States should also include these considerations into their national cybersecurity framework, notably through strategies, laws, regulations and other administrative provisions.

REAL-TIME REQUIREMENTS OF ENERGY INFRASTRUCTURE COMPONENTS

(3) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to real-time requirements in the energy sector. Some elements of the energy system need to work under 'real time', that is to say reacting to commands within a few milliseconds, which makes it difficult or even impossible to introduce cybersecurity measures due to a lack of time.

(4) In particular, energy network operators should:

(a) apply the most recent security standards for new installations wherever adequate and consider complementary physical security measures where the installed base of old installations cannot be sufficiently protected by cybersecurity mechanisms;

(b) implement international standards on cybersecurity and adequate specific technical standards for secure real- time communication as soon as respective products become commercially available;

(c) consider real-time constraints in the overall security concept for assets, especially in asset classification;

(d) consider privately owned networks for tele-protection schemes to ensure the quality of service level required for real-time constraints; when using public communication networks, operators should consider ensuring specific bandwidth allocation, latency requirements and communication security measures;

(e) split the overall system into logical zones and within each zone, define time and process constraints in order to enable the application of suitable cybersecurity measures or to consider alternative protection methods.

(5) Where available, energy network operators should also:

(a) choose a secure communication protocol, taking into consideration real-time requirements, for example between an installation and its management systems (Energy Management System - EMS/Distribution Management System - DMS);

(b) introduce an appropriate authentication mechanism for machine-to-machine communication, addressing real- time requirements.

CASCADING EFFECTS

(6) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to cascading effects in the energy sector. Electricity grids and gas pipelines are strongly interconnected across Europe and a cyber-attack creating an outage or disruption in a part of the energy system might trigger far-reaching cascading effects into other parts of that system.

(7) In applying this Recommendation, Member States should evaluate the interdependencies and criticality of power generation and flexible-demand systems, transmission and distribution substations and lines, and the associated impacted stakeholders (including cross-border situations) in case of a successful cyber-attack or cyber incident. Member States should also ensure that energy network operators have a communication framework with all key stakeholders to share early warning signs and cooperate on crisis management. There should be structured communication channels and agreed formats in place in order to share sensitive information with all relevant stakeholders, Computer Security Incident Response Teams, and relevant authorities.

(8) In particular, energy network operators should:

(a) ensure that new devices, including internet of Things devices, have and will maintain a level of cybersecurity appropriate to a site's criticality;

(b) adequately consider cyber-physical effects when establishing and periodically reviewing business continuity plans;

(c) establish design criteria and an architecture for a resilient grid, which could be achieved by:

- putting in place in-depth defence measures per site, tailored to a site's criticality,

- identifying critical nodes, both in terms of power production capacity and customer impact; Critical functions of a grid should be designed to mitigate risk that can cause cascading effects by considering redundancy, resilience to phase oscillations and protections against cascaded load cut-off,

- collaborating with other relevant operators and with technology suppliers to prevent cascading effects by applying appropriate measures and services,

- designing and building communication and control networks with a view to confining the effects of any physical and logical failures to limited parts of the networks and to ensuring adequate and swift mitigation measures.

LEGACY AND STATE-OF-THE-ART TECHNOLOGY

(9) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to the combination of legacy and state-of-the-art technology in the energy sector. Indeed, two different types of technologies co-exist in today's energy system: an older technology with a lifespan of 30 to 60 years, designed before cybersecurity considerations, and modern equipment, reflecting state-of-the-art digitalisation and smart devices.

(10) In applying this Recommendation, Member States should encourage energy network operators and technology suppliers to follow the relevant internationally accepted standards on cybersecurity wherever possible. Meanwhile, stakeholders and customers should adopt a cybersecurity-oriented approach when connecting devices to the grid.

(11) In particular, technology suppliers should provide tested solutions for security issues in legacy or new technologies free of charge and as soon as a relevant security issue becomes known.

(12) In particular, energy network operators should:

(a) analyse the risks of connecting legacy and internet of Things concepts and be aware about internal and external interfaces and their vulnerabilities;

(b) take suitable measures against malicious attacks originating from large numbers of maliciously controlled consumer devices or applications;

(c) establish an automated monitoring and analysis capability for security-related events in legacy and internet of Things environments, such as unsuccessful attempts to log-in, door alarms for cabinet opening or other events;

(d) conduct on a regular basis specific cybersecurity risk analysis on all legacy installations, especially when connecting old and new technologies; since the legacy installations often represent a very large number of assets, risk analysis might be done by asset classes;

(e) update software and hardware of legacy and internet of Things systems to the most recent version whenever adequate; in so doing, energy network operators should consider complementary measures such as system segregation or adding external security barriers where patching or updating would be adequate but is not possible, for instance unsupported products;

(f) formulate tenders with cybersecurity in mind, that is to say demand information about security features, demand compliance with existing cybersecurity standards, ensure continuous alerting, patching and mitigation proposals if vulnerabilities are discovered, and clarify vendor liability in the event of cyber-attacks or incidents;

(g) collaborate with technology suppliers to replace legacy systems whenever beneficial for security reasons, but take into account critical system functionalities.

MONITORING

(13) Member States should communicate to the Commission, within 12 months after the adoption of this Recommendation, and every two years thereafter, detailed information regarding the state of implementation of this Recommendation through the NIS Cooperation Group.

REVIEW

(14) On the basis of the information submitted by the Member States, the Commission will review the implementation of this Recommendation and assess whether further measures are required as appropriate in consultation with the Member States and the relevant stakeholders.

ADDRESSEES

(15) This Recommendation is addressed to the Member States.

(…)

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

(…)

Whereas:

(1) The electricity sector in the Union is undergoing a profound transformation, characterised by more decentralised markets with more players, a higher proportion of energy from renewable sources and better interconnected systems. In response, Regulation (EU) 2019/943 of the European Parliament and of the Council and Directive (EU) 2019/944 of the European Parliament and of the Council aim to upgrade the legal framework governing the Union's internal electricity market, in order to ensure that markets and networks function in an optimal manner, to the benefit of businesses and Union citizens. This Regulation is intended to contribute to the implementation of the objectives of the Energy Union, of which energy security, solidarity, trust and an ambitious climate policy are an integral part.

(2) Well-functioning markets and systems, with adequate electricity interconnections, are the best guarantee of security of electricity supply. However, even where markets and systems function well and are interconnected, the risk of an electricity crisis, as a result of natural disasters, such as extreme weather conditions, malicious attacks or fuel shortages, can never be excluded. The consequences of electricity crises often extend beyond national borders. Even where such crises start locally, their effects can rapidly spread across borders. Some extreme circumstances, such as cold spells, heat waves or cyberattacks, may affect entire regions at the same time.

(3) In a context of interlinked electricity markets and systems, electricity crisis prevention and management cannot be considered to be a purely national task. The potential of more efficient and less costly measures through regional cooperation should be better exploited. A common framework of rules and better coordinated procedures are needed in order to ensure that Member States and other actors are able to cooperate effectively across borders, in a spirit of increased transparency, trust and solidarity between Member States.

(4) Directive 2005/89/EC of the European Parliament and of the Council established the necessary measures that the Member States are to take in order to ensure security of electricity supply in general. The provisions of that Directive have largely been superseded by subsequent legislative acts, in particular as regards how electricity markets are to be organised in order to

ensure the availability of sufficient capacity, how transmission system operators are to cooperate to guarantee system stability, and as regards ensuring that appropriate infrastructure is in place. This Regulation addresses the specific issue of electricity crisis prevention and management.

(5) Commission Regulations (EU) 2017/1485 and (EU) 2017/2196 constitute a detailed rulebook governing how transmission system operators and other relevant stakeholders should act and cooperate to ensure system security. Those technical rules should ensure that most electricity incidents are dealt with effectively at operational level. This Regulation focuses on electricity crises that have a larger scale and impact. It sets out what Member States should do to prevent such crises and what measures they can take should system operation rules alone no longer suffice. Even in electricity crises system operation rules should continue to be fully respected and this Regulation should be consistent with Regulation (EU) 2017/2196.

(6) This Regulation sets out a common framework of rules on how to prevent, prepare for and manage electricity crises, bringing more transparency in the preparation phase and during an electricity crisis and ensuring that measures are taken in a coordinated and effective manner. It requires Member States to cooperate, at regional level and, where applicable, bilaterally, in a spirit of solidarity. It also sets out a framework for the effective monitoring of security of electricity supply in the Union via the Electricity Coordination Group (ECG), which was set up by a Commission Decision of 15 November 2012 as a forum in which to exchange information and foster cooperation among Member States, in particular in the area of security of electricity supply. Member State cooperation and the monitoring framework are intended to achieve better risk-preparedness at a lower cost. This Regulation should also strengthen the internal electricity market by enhancing trust and confidence across Member States and ruling out inappropriate state interventions in electricity crises, in particular avoiding undue curtailment of cross-border flows and cross zonal transmission capacities, thus reducing the risk of negative spillover effects on neighbouring Member States.

(7) Directive (EU) 2016/1148 of the European Parliament and of the Council lays down general rules on security of network and information systems, while specific rules on cybersecurity will be developed through a network code as laid down in Regulation (EU) 2019/943. This Regulation complements Directive (EU) 2016/1148 by ensuring that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans.

(8) Council Directive 2008/114/EC lays down a process with a view to enhancing the security of designated European critical infrastructure, including certain electricity infrastructure. Directive 2008/114/EC, together with this Regulation, contributes to creating a comprehensive approach to the energy security of the Union.

(9) Decision No 1313/2013/EU of the European Parliament and of the Council sets out requirements for Member States to develop risk assessments at national level or at the appropriate sub-national level every three years, and to develop and refine their disaster risk management planning at national level or at the appropriate sub-national level. The specific risk prevention, preparedness and planning actions set out in this Regulation should be consistent with the wider, multi-hazard national risk assessments required under Decision No 1313/2013/EU.

(10) Member States are responsible for ensuring the security of electricity supply within their territories, while security of electricity supply is also a responsibility shared among the Commission and other Union actors, within their respective areas of activity and competence. Security of electricity supply entails effective cooperation among Member States, Union institutions, bodies, offices and agencies, and relevant stakeholders. Distribution system operators and transmission system operators play a key role in ensuring a secure, reliable and efficient electricity system in accordance with Articles 31 and 40 of Directive (EU) 2019/944. The regulatory authorities and other relevant national authorities also play an important role in

ensuring and monitoring the security of electricity supply, as part of their tasks attributed by Article 59 of Directive (EU) 2019/944. Member States should designate an existing or new entity as their single competent national governmental or regulatory authority with the aim of ensuring the transparent and inclusive participation of all actors involved, the efficient preparation and proper implementation of the risk-preparedness plans, as well as facilitating the prevention and *ex post* evaluation of electricity crises and information exchanges in relation thereto.

(11) A common approach to electricity crisis prevention and management requires a common understanding among Member States as to what constitutes an electricity crisis. In particular this Regulation should facilitate coordination among Member States for the purpose of identifying a situation in which the potential risk of a significant electricity shortage or an impossibility to supply electricity to customers is present or imminent. The European Network of Transmission System Operators for Electricity ('ENTSO for Electricity') and the Member States should, respectively, determine concrete regional and national electricity crisis scenarios. That approach should ensure that all relevant electricity crises are covered, taking into account regional and national specificities such as the topology of the grid, the electricity mix, the size of production and consumption, and the degree of population density.

(12) A common approach to electricity crisis prevention and management also requires that Member States use the same methods and definitions to identify risks relating to the security of electricity supply and are in a position to compare effectively how well they and their neighbours perform in that area. This Regulation identifies two indicators for monitoring the security of electricity supply in the Union: 'expected energy non-served', expressed in GWh/year, and 'loss of load expectation', expressed in hours per year. Those indicators are part of the European resource adequacy assessment carried out by the ENTSO for Electricity, pursuant to Article 23 of Regulation (EU) 2019/943. The ECG should carry out regular monitoring of the security of electricity supply based on the results of those indicators. The Agency for the Cooperation of Energy Regulators (ACER) should also use those indicators when reporting on Member States' performance in the area of security of electricity supply in its annual electricity market monitoring reports, pursuant to Article 15 of Regulation (EU) 2019/942 of the European Parliament and of the Council.

(13) To ensure the coherence of risk assessments in a manner that builds trust between Member States in an electricity crisis, a common approach to identifying risk scenarios is needed. The ENTSO for Electricity should therefore, after consulting the relevant stakeholders, develop and update a common methodology for risk identification in cooperation with ACER, and with the ECG in its formation composed only of representatives of the Member States. The ENTSO for Electricity should propose the methodology and ACER should approve it. When consulting the ECG, ACER is to take the utmost account of the views expressed by the ECG. The ENTSO for Electricity should update the common methodology for risk identification where significant new information becomes available.

(14) On the basis of the common methodology for risk identification, the ENTSO for Electricity should regularly draw up and update regional electricity crisis scenarios and identify the most relevant risks for each region such as extreme weather conditions, natural disasters, fuel shortages or malicious attacks. When considering the crisis scenario of a gas fuel shortage, the risk of disruption of the gas supply should be assessed based on the gas supply and infrastructure disruption scenarios developed by the European Network of Transmission System Operators for Gas (ENTSOG) pursuant to Article 7 of Regulation (EU) 2017/1938 of the European Parliament and of the Council (14). The ENTSO for Electricity should be able to delegate tasks relating to the identification of regional electricity crisis scenarios to regional coordination centres established pursuant to Article 35 of Regulation (EU) 2019/943. Those delegated tasks should be performed under the supervision of the ENTSO for Electricity. Member States should establish and update their national electricity crisis scenarios on the basis of regional electricity crisis scenarios, in principle every four years. Those scenarios should provide the basis for the risk-preparedness

plans. When identifying risks at national level, the Member States should describe any risks that they identify in relation to the ownership of the infrastructure relevant for security of electricity supply and any measures taken to address those risks such as general or sector-specific investment screening laws, special rights for certain shareholders, with an indication why they consider such measures to be necessary and proportionate.

(15) A regional approach to identifying risk scenarios and to developing preventive, preparatory and mitigating measures should bring significant benefits in terms of the effectiveness of those measures and the optimal use of resources. Moreover, in a simultaneous electricity crisis, a coordinated and pre-agreed approach would ensure a consistent response and reduce the risk of negative spillover effects that purely national measures could have in neighbouring Member States. This Regulation therefore requires Member States to cooperate in a regional context.

(16) The regional coordination centres should perform the tasks of regional relevance assigned to them in accordance with Regulation (EU) 2019/943. To ensure that they can carry out their tasks effectively and act in close cooperation with relevant national authorities with a view to preventing and mitigating larger-scale electricity incidents, the regional cooperation required under this Regulation should build on the regional cooperation structures used at technical level, namely the groups of Member States sharing the same regional coordination centre. The geographical regions of the regional coordination centres are therefore relevant for the identification of the regional electricity crisis scenarios and risk assessments. However, Member States should have the possibility to form subgroups within the regions for the purpose of cooperation with regard to concrete regional measures, or to cooperate in existing regional cooperation forums for that purpose, as the technical ability to provide mutual assistance to each other in an electricity crisis is essential. This is because not all Member States in a larger region will necessarily be able to provide electricity to another Member State in an electricity crisis. Thus, it is not necessary for all Member States in a region to conclude regional agreements on concrete regional measures. Instead, Member States that have the technical ability to provide assistance to each other should conclude such agreements.

(17) Regulation (EU) 2019/943 provides for the use of a common methodology for the medium to long-term European resource adequacy assessment (from 10-year-ahead to year-ahead), with a view to ensuring that Member States' decisions as to possible investment needs are made on a transparent and commonly agreed basis. The European resource adequacy assessment has a different purpose from the short-term adequacy assessments which are used to detect possible adequacy related problems in short time-frames, namely seasonal adequacy assessments (six months ahead) and week-ahead to at least day-ahead adequacy assessments. Regarding short-term assessments, there is a need for a common approach to the way possible adequacy-related problems are detected. The ENTSO for Electricity should carry out winter and summer adequacy assessments to alert Member States and transmission system operators to risks related to the security of electricity supply that might occur in the following six months. To improve those adequacy assessments, the ENTSO for Electricity should develop a common probabilistic methodology for them, after consulting the relevant stakeholders, and in cooperation with ACER, and with the ECG, in its formation composed only of representatives of the Member States. The ENTSO for Electricity should propose that methodology and updates thereto to ACER, and ACER should approve the proposal and the updates. When consulting the ECG, ACER is to take the utmost account of the views expressed by the ECG. The ENTSO for Electricity should update the methodology where significant new information becomes available. The ENTSO for Electricity should be able to delegate tasks relating to seasonal adequacy assessments to regional coordination centres, while delegated tasks should be performed under the ENTSO for Electricity's supervision.

(18) Transmission system operators should apply the methodology used to prepare seasonal adequacy assessments when carrying out any other type of short-term risk assessment, namely

the week-ahead to at least day-ahead generation adequacy forecasts provided for in Regulation (EU) 2017/1485.

(19) To ensure a common approach to electricity crisis prevention and management, the competent authority of each Member State should draw up a risk-preparedness plan on the basis of the regional and national electricity crisis scenarios. The competent authorities should consult stakeholders or representatives of stakeholder groups, such as representatives of producers or their trade bodies or of distribution system operators, where they are relevant for the prevention and handling of an electricity crisis. To that end, the competent authorities should decide on the appropriate arrangements for carrying out the consultation. The risk-preparedness plans should describe effective, proportionate and non-discriminatory measures addressing all identified electricity crisis scenarios. The environmental impact of demand-side and supply-side measures proposed should be taken into account. The plans should provide transparency especially as regards the conditions in which non-market-based measures can be taken to mitigate electricity crises. All envisaged non-market-based measures should comply with the rules laid down in this Regulation. The risk-preparedness plans should be made public, while ensuring confidentiality of sensitive information.

(20) The risk-preparedness plans should set out national, regional and, where applicable, bilateral measures. Regional and, where applicable, bilateral measures are necessary, in particular in the event of a simultaneous electricity crisis, when a coordinated and pre-agreed approach is needed to ensure a consistent response and reduce the risk of negative spillover effects. To that end, before adopting the risk-preparedness plans, competent authorities should consult the competent authorities of the relevant Member States. The relevant Member States are those where there could be negative spillover effects or other impacts on each other's electricity system, whether those Member States are in the same region or directly connected. The plans should take account of the relevant national circumstances, including the situation of outermost regions within the meaning of Article 349 of the Treaty on the Functioning of the European Union, and of some micro-isolated systems that are not connected to the national transmission systems. In that respect, Member States should draw the appropriate conclusions as regards, inter alia, the provisions of this Regulation on identification of regional electricity crisis scenarios and the regional and bilateral measures set out in risk-preparedness plans as well as provisions on assistance. The plans should clearly set out the roles and responsibilities of the competent authorities. National measures should take full account of the regional and bilateral measures that have been agreed and should take full advantage of the opportunities provided by regional cooperation. The plans should be technical and operational in nature, their function being to help prevent the occurrence or escalation of an electricity crisis and to mitigate its effects.

(21) The risk-preparedness plans should be updated regularly. To ensure that the plans are up-to-date and effective, the competent authorities of the Member States of each region should organise biennial simulations of electricity crises in cooperation with transmission system operators and other relevant stakeholders in order to test their suitability.

(22) The template provided for in this Regulation is intended to facilitate the preparation of the plans, allowing for the inclusion of additional, Member State specific information. The template is also intended to facilitate consultation of other Member States in the region concerned and the ECG. Consultation within the region and within the ECG should ensure that measures taken in one Member State or region do not put at risk the security of electricity supply of other Member States or regions.

(23) It is important to facilitate communication and transparency between Member States, where they have concrete, serious and reliable information that an electricity crisis may occur. In such circumstances the Member States concerned should inform the Commission, the neighbouring Member States and the ECG without undue delay, providing, in particular, information on the causes of the deterioration of the electricity supply situation, the planned measures to prevent the electricity crisis and the possible need for assistance from other Member States.

(24) Information exchange in the event of an electricity crisis is essential in order to ensure coordinated action and targeted assistance. Therefore, this Regulation obliges the competent authority to inform the Member States in the region, the neighbouring Member States and the Commission without undue delay when confronted with an electricity crisis. The competent authority should also provide information on the causes of the crisis, the measures planned or taken to mitigate the crisis and the possible need for assistance from other Member States. Where that assistance goes beyond security of electricity supply, the Union Civil Protection Mechanism should remain the applicable legal framework.

(25) In the event of an electricity crisis Member States should cooperate in a spirit of solidarity. In addition to that general rule, appropriate provision should be made for Member States to offer each other assistance in an electricity crisis. Such assistance should be based on agreed, coordinated measures set out in the risk-preparedness plans. This Regulation gives Member States a wide discretion when agreeing on the content of such coordinated measures and thus on the content of the assistance that they offer. It is for Member States to decide and agree on such coordinated measures, taking into account demand and supply. At the same time, this Regulation ensures that, for the purpose of the agreed assistance, electricity is delivered in a coordinated manner. Member States should agree on the necessary technical, legal and financial arrangements for the implementation of the regional and bilateral measures that have been agreed. Under those technical arrangements the Member States should indicate the maximum quantities of electricity to be delivered, which should be re-assessed on the basis of the technical feasibility of delivering electricity once the assistance is required during an electricity crisis. Subsequently, Member States should take all necessary measures for the implementation of the regional and bilateral measures that have been agreed and technical, legal and financial arrangements.

(26) When agreeing on coordinated measures and technical, legal and financial arrangements and otherwise implementing provisions on assistance, Member States should take account of social and economic factors, including the security of Union citizens, and proportionality. They are encouraged to exchange best practices and to use the ECG as a discussion platform through which to identify the available options for assistance, in particular concerning coordinated measures and the necessary technical, legal and financial arrangements, including fair compensation. The Commission may facilitate the preparation of the regional and bilateral measures.

(27) Assistance between Member States under this Regulation should be subject to fair compensation agreed between the Member States. This Regulation does not harmonise all aspects of such fair compensation between Member States. The Member States should therefore agree on provisions on fair compensation before assistance is provided. The Member State requesting assistance should promptly pay, or ensure the prompt payment of, such compensation to the Member State providing the assistance. The Commission should provide for non-binding guidance on the key elements of fair compensation and other elements of the technical, legal and financial arrangements.

(28) In providing assistance under this Regulation, Member States implement Union law and are therefore bound to respect fundamental rights guaranteed by Union law. Such assistance may therefore, depending on the measures agreed between Member States, give rise to an obligation on a Member State to pay compensation to those affected by its measures. Member States should therefore, where necessary, ensure that national compensation rules which comply with Union law, in particular with fundamental rights, are in place. Moreover, the Member State that receives assistance should ultimately bear all the reasonable costs that another Member State incurs as a result of providing assistance pursuant to such national compensation rules.

(29) In the event of an electricity crisis, assistance should be provided even if Member States have not yet agreed on coordinated measures and technical, legal and financial arrangements as required by the provisions of this Regulation on assistance. In order to be able to provide assistance in such a situation in accordance with this Regulation, Member States should agree on

ad hoc measures and arrangements in place of the absent coordinated measures and technical, legal and financial arrangements.

(30) This Regulation introduces such an assistance mechanism between Member States as an instrument to prevent or mitigate an electricity crisis within the Union. The Commission should therefore review the assistance mechanism in light of future experience with its functioning, and propose, where appropriate, modifications thereto.

(31) This Regulation should enable electricity undertakings and customers to rely on the market mechanisms laid down in Regulation (EU) 2019/943 and Directive (EU) 2019/944 for as long as possible when coping with electricity crises. Rules governing the internal market and system operation rules should be complied with even in electricity crises. Such rules include point (i) of Article 22(1) of Regulation (EU) 2017/1485 and Article 35 of Regulation (EU) 2017/2196, which govern transaction curtailment, limitation of provision of cross zonal capacity for capacity allocation or limitation of provision of schedules. This means that non-market-based measures, such as forced demand disconnection, or the provision of extra supplies outside normal market functioning should be taken only as a last resort, when all possibilities provided by the market have been exhausted. Therefore, forced demand disconnection should be introduced only after all possibilities for voluntary demand disconnection have been exhausted. In addition, any non-market-based measures should be necessary, proportionate, non-discriminatory and temporary.

(32) In order to ensure transparency after an electricity crisis, the competent authority that declared the electricity crisis should carry out an *ex post* evaluation of the crisis and its impact. That evaluation should take into account, inter alia, the effectiveness and proportionality of the measures taken as well as their economic cost. That evaluation should also cover cross-border considerations, such as the impact of the measures on other Member States and the level of the assistance that the Member State that declared the electricity crisis received from them.

(33) The transparency obligations should ensure that all measures that are taken to prevent or manage electricity crises comply with internal market rules and are in line with the principles of cooperation and solidarity which underpin the Energy Union.

(34) This Regulation reinforces the role of the ECG. It should carry out specific tasks, in particular in connection with the development of a methodology for identifying regional electricity crisis scenarios and a methodology for short-term and seasonal adequacy assessments and in connection with the preparation of the risk-preparedness plans, and should have a prominent role in monitoring Member States' performance in the area of the security of electricity supply, and developing best practices on that basis.

(35) It is possible that an electricity crisis extends beyond Union borders to the territory of the Energy Community Contracting Parties. As a party to the Treaty establishing the Energy Community, the Union should promote amendments to that Treaty with the aim of creating an integrated market and a single regulatory space by providing an appropriate and stable regulatory framework. In order to ensure efficient crisis management, the Union should closely cooperate with the Energy Community Contracting Parties when preventing, preparing for and managing an electricity crisis.

(36) Where the Commission, ACER, the ECG, the ENTSO for Electricity, Member States and their competent and regulatory authorities, or any other bodies, entities or persons, receive confidential information pursuant to this Regulation, they should ensure the confidentiality of that information. To that end, confidential information should be subject to Union and national rules in place on the handling of confidential information and processes.

(37) Since the objective of this Regulation, namely to ensure the most effective and efficient risk-preparedness within the Union, cannot be sufficiently achieved by Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European

Union. In accordance with the principle of proportionality set out in that Article, this Regulation does not go beyond what is necessary to achieve that objective.

(38) Cyprus is currently the only Member State which is not directly connected to another Member State. It should be clarified with respect to certain provisions of this Regulation that, for as long as this situation persists, those provisions, namely provisions on the identification of regional electricity crisis scenarios, on including regional and bilateral measures set out in risk-preparedness plans, and on assistance, do not apply with respect to Cyprus. Cyprus and relevant other Member States are encouraged to develop, with the support of the Commission, alternative measures and procedures in the fields covered by those provisions, provided that such alternative measures and procedures do not affect the effective application of this Regulation between the other Member States.

(…)

CHAPTER I

General Provisions

Article 1. Subject matter
This Regulation lays down rules for cooperation between Member States with a view to preventing, preparing for and managing electricity crises in a spirit of solidarity and transparency and in full regard for the requirements of a competitive internal market for electricity.

Article 2. Definitions
For the purposes of this Regulation, the following definitions apply:

(1) ‘ security of electricity supply ’means the ability of an electricity system to guarantee the supply of electricity to customers with a clearly established level of performance, as determined by the Member States concerned;

(2) ‘ transmission system operator ’means transmission system operator as defined in point (35) of Article 2 of Directive (EU) 2019/944;

(3) ‘ distribution ’means distribution as defined in point (28) of Article 2 of Directive (EU) 2019/944;

(4) ‘ cross-border flow ’means cross-border flow as defined in point (3) of Article 2 of Regulation (EU) 2019/943;

(5) ‘ cross zonal capacity ’means the capability of the interconnected system to accommodate energy transfer between bidding zones;

(6) ‘ customer ’means customer as defined in point (1) of Article 2 of Directive (EU) 2019/944;

(7) ‘ distribution system operator ’means distribution system operator as defined in point (29) of Article 2 of Directive (EU) 2019/944;

(8) ‘ generation ’means generation as defined in point (37) of Article 2 of Directive (EU) 2019/944;

(9) ‘ electricity crisis ’means a present or imminent situation in which there is a significant electricity shortage, as determined by the Member States and described in their risk-preparedness plans, or in which it is impossible to supply electricity to customers;

(10) ‘ simultaneous electricity crisis ’means an electricity crisis affecting more than one Member State at the same time;

(11) ‘ competent authority ’means a national governmental authority or a regulatory authority designated by a Member State in accordance with Article 3;

(12) ‘ regulatory authorities ’means regulatory authorities referred to in Article 57(1) of Directive (EU) 2019/944;

(13) ‘ crisis coordinator ’means a person, a group of persons, a team composed of the relevant national electricity crisis managers or an institution tasked with acting as a contact point and coordinating the information flow during an electricity crisis;

(14) ‘ non-market-based measure ’means any supply- or demand-side measure that deviates from market rules or commercial agreements, the purpose of which is to mitigate an electricity crisis;

(15) ‘ producer ’means producer as defined in point (38) of Article 2 of Directive (EU) 2019/944;

(16) ‘ region ’means a group of Member States whose transmission system operators share the same regional coordination centre as referred to in Article 36 of Regulation (EU) 2019/943;

(17) ‘ subgroup ’means a group of Member States, within a region, which have the technical ability to provide each other assistance in accordance with Article 15;

(18) ‘ early warning ’means a provision of concrete, serious, reliable information indicating that an event may occur which is likely to result in a significant deterioration of the electricity supply situation and is likely to lead to electricity crisis;

(19) ‘ transmission ’means transmission as defined in point (34) of Article 2 of Directive (EU) 2019/944;

(20) ‘ electricity undertaking ’means electricity undertaking as defined in point (57) of Article 2 of Directive (EU) 2019/944;

(21) ‘ capacity allocation ’means the attribution of cross zonal capacity;

(22) ‘ energy from renewable sources ’means energy from renewable sources or renewable energy as defined in point (31) of Article 2 of Directive (EU) 2019/944.

Article 3. Competent authority

1. As soon as possible and in any event by 5 January 2020, each Member State shall designate a national governmental or regulatory authority as its competent authority. The competent authorities shall be responsible for, and shall cooperate with each other for the purposes of, carrying out the tasks provided for in this Regulation. Where appropriate, until the competent authority has been designated, the national entities responsible for the security of electricity supply shall carry out the tasks of the competent authority in accordance with this Regulation.

2. Member States shall, without delay, notify the Commission and the ECG and make public the name and the contact details of their competent authorities designated pursuant to paragraph 1 and any changes to their name or contact details.

3. Member States may allow the competent authority to delegate the operational tasks regarding risk-preparedness planning and risk management set out in this Regulation to other bodies. Delegated tasks shall be performed under the supervision of the competent authority and shall be specified in the risk-preparedness plan in accordance with point (b) of Article 11(1).

CHAPTER II

Risk assessment

Article 4. Assessment of risks to security of electricity supply

Each competent authority shall ensure that all relevant risks relating to security of electricity supply are assessed in accordance with the rules laid down in this Regulation and in Chapter IV of

Regulation (EU) 2019/943. To that end, it shall cooperate with transmission system operators, distribution system operators, regulatory authorities, the ENTSO for Electricity, regional coordination centres and other relevant stakeholders, as required.

Article 5. Methodology for identifying regional electricity crisis scenarios

1. By 5 January 2020, the ENTSO for Electricity shall submit to ACER a proposal for a methodology for identifying the most relevant regional electricity crisis scenarios.

2. The proposed methodology shall identify electricity crisis scenarios in relation to system adequacy, system security and fuel security on the basis of at least the following risks:

(a) rare and extreme natural hazards;

(b) accidental hazards going beyond the N-1 security criterion and exceptional contingencies;
(c) consequential hazards including the consequences of malicious attacks and of fuel shortages.

3. The proposed methodology shall include at least the following elements:

(a) a consideration of all relevant national and regional circumstances, including any subgroups;

(b) interaction and correlation of risks across borders;

(c) simulations of simultaneous electricity crisis scenarios;

(d) ranking of risks according to their impact and probability;

(e) principles on how to handle sensitive information in a manner that ensures transparency towards the public.

4. When considering the risks of disruption of gas supply in the context of identifying the risks pursuant to point (c) of paragraph 2 of this Article, the ENTSO for Electricity shall use the natural gas supply and infrastructure disruption scenarios developed by ENTSOG pursuant to Article 7 of Regulation (EU) 2017/1938.

5. Before submitting the proposed methodology to ACER, the ENTSO for Electricity shall conduct a consultation involving at least the regional coordination centres, industry and consumer organisations, producers or their trade bodies, transmission system operators and relevant distribution system operators, competent authorities, regulatory authorities and other relevant national authorities. The ENTSO for Electricity shall duly take into account the results of the consultation and present them, together with the proposed methodology, at a meeting of the ECG.

6. Within two months of receipt of the proposed methodology, ACER shall, after consulting the ECG, in its formation composed only of representatives of the Member States, approve or amend the proposal. The ENTSO for Electricity and ACER shall publish the final version of the methodology on their websites.

7. The ENTSO for Electricity shall update and improve the methodology in accordance with paragraphs 1 to 6 where significant new information becomes available. The ECG in its formation composed only of representatives of the Member States may recommend, and ACER or the Commission may request, such updates and improvements with due justification. Within six months of receipt of the request, the ENTSO for Electricity shall submit to ACER a draft of the proposed changes. Within two months of receipt of such a draft, ACER shall, after consulting the ECG, in its formation composed only of representatives of the Member States, approve or amend the proposed changes. The ENTSO for Electricity and ACER shall publish the final version of the

Article 6. Identification of regional electricity crisis scenarios
1. Within six months of the approval of a methodology pursuant to Article 5(6), the ENTSO for Electricity shall, on the basis of that methodology and in close cooperation with the ECG, regional coordination centres, competent authorities and regulatory authorities, identify the most relevant electricity crisis scenarios for each region. It may delegate tasks relating to the identification of regional electricity crisis scenarios to the regional coordination centres.

2. The ENTSO for Electricity shall submit the regional electricity crisis scenarios to the relevant transmission system operators, regional coordination centres, competent authorities and regulatory authorities as well as to the ECG. The ECG may recommend amendments.

3. The ENTSO for Electricity shall update the regional electricity crisis scenarios every four years, unless circumstances warrant more frequent updates.

Article 7. Identification of national electricity crisis scenarios
1. Within four months of the identification of the regional electricity crisis scenarios in accordance with Article 6(1), the competent authority shall identify the most relevant national electricity crisis scenarios.

2. In identifying the national electricity crisis scenarios, the competent authority shall consult the transmission system operators, the distribution system operators that the competent authority considers to be relevant, the relevant producers or their trade bodies, and the regulatory authority where it is not the competent authority.

3. The national electricity crisis scenarios shall be identified on the basis of at least the risks referred to in Article 5(2) and shall be consistent with the regional electricity crisis scenarios identified in accordance with Article 6(1). Member States shall update the national electricity crisis scenarios every four years, unless circumstances warrant more frequent updates.

4. Within four months of identification of regional electricity crisis scenarios in accordance with Article 6(1), Member States shall inform the ECG and the Commission of their assessment of the risks in relation to the ownership of infrastructure relevant for security of electricity supply, and any measures taken to prevent or mitigate such risks, with an indication of why such measures are considered necessary and proportionate.

Article 8. Methodology for short-term and seasonal adequacy assessments
1. By 5 January 2020, the ENTSO for Electricity shall submit to ACER a proposal for a methodology for assessing seasonal and short-term adequacy, namely monthly, week-ahead to at least day-ahead adequacy, which shall cover at least the following:

(a) the uncertainty of inputs such as the probability of a transmission capacity outage, the probability of an unplanned outage of power plants, severe weather conditions, variable demand, in particular peaks depending on weather conditions, and variability of production of energy from renewable sources;

(b) the probability of the occurrence of an electricity crisis;

(c) the probability of the occurrence of a simultaneous electricity crisis.

2. The methodology referred to in paragraph 1 shall provide for a probabilistic approach, including multiple scenarios, and shall take into account the national, regional and Union context, including the level of interconnection between Member States and, to the extent possible, third countries within synchronous areas of the Union. The methodology shall take into account the specificities of each Member State's energy sector, including specific weather conditions and external circumstances.

3. Before submitting the proposed methodology, the ENTSO for Electricity shall conduct a consultation involving at least the regional coordination centres, industry and consumer organisations, producers or their trade bodies, transmission system operators, relevant distribution system operators, competent authorities, regulatory authorities and other relevant national authorities. The ENTSO for Electricity shall duly take into account the results of the consultation and present them, together with the proposed methodology, at a meeting of the ECG.

4. Within two months of receipt of the proposed methodology, ACER shall, after consulting the ECG in its formation composed only of representatives of the Member States, approve or amend the proposal. The ENTSO for Electricity and ACER shall publish the final version of the methodology on their websites.

5. The ENTSO for Electricity shall update and improve the methodology in accordance with paragraphs 1 to 4 where significant new information becomes available. The ECG in its formation composed only of representatives of the Member States may recommend, and ACER or the Commission may request, such updates and improvements with due justification. Within six months of receipt of the request, the ENTSO for Electricity shall submit to ACER a draft of the proposed changes. Within two months of receipt of such a draft, ACER shall, after consulting the ECG, in its formation composed only of representatives of the Member States, approve or amend the proposed changes. The ENTSO for Electricity and ACER shall publish the final version of the updated methodology on their websites.

Article 9. Short-term and seasonal adequacy assessments

1. All short-term adequacy assessments, whether carried out at national, regional or Union level, shall be carried out in accordance with the methodology developed pursuant to Article 8.

2. The ENTSO for Electricity shall carry out seasonal adequacy assessments in accordance with the methodology developed pursuant to Article 8. It shall publish the results for the winter adequacy assessment by 1 December each year and for the summer adequacy assessment by 1 June each year. It may delegate tasks relating to the adequacy assessments to regional coordination centres. It shall present the adequacy assessment at a meeting of the ECG, which may make recommendations where appropriate.

3. The regional coordination centres shall carry out week-ahead to at least day ahead adequacy assessments in accordance with Regulation (EU) 2017/1485 on the basis of the methodology adopted pursuant to Article 8 of this Regulation.

CHAPTER III

Risk-preparedness plans

Article 10. Establishment of risk-preparedness plans

1. On the basis of the regional and national electricity crisis scenarios identified pursuant to Articles 6 and 7, the competent authority of each Member State shall establish a risk-preparedness plan, after consulting distribution system operators considered relevant by the competent authority, the transmission system operators, the relevant producers or their trade bodies, the electricity and natural gas undertakings, the relevant organisations that represent the interests of industrial and non-industrial electricity customers, and the regulatory authority where it is not the competent authority.

2. The risk-preparedness plan shall consist of national measures, regional and, where applicable, bilateral measures as provided for in Articles 11 and 12. In accordance with Article 16, all measures that are planned or taken to prevent, prepare for and mitigate electricity crises shall fully comply with the rules governing the internal electricity market and system operation. Those measures shall be clearly defined, transparent, proportionate and non-discriminatory.

3. The risk-preparedness plan shall be developed in accordance with Articles 11 and 12 and with the template set out in the Annex. If necessary, Member States may include additional information in the risk-preparedness plan.

4. In order to ensure consistency of risk-preparedness plans, competent authorities shall, before adopting their risk-preparedness plans, submit the draft plans, for consultation, to the competent authorities of the relevant Member States in the region and, where they are not in the same region, to the competent authorities of directly connected Member States, as well as to the ECG.

5. Within six months of receipt of the draft risk-preparedness plans, the competent authorities referred to in paragraph 4 and the ECG may issue recommendations relating to the draft plans submitted pursuant to paragraph 4.

6. Within nine months of submitting their draft plans, the competent authorities concerned shall adopt their risk-preparedness plans, taking into account the results of the consultation pursuant to paragraph 4 and any recommendations issued pursuant to paragraph 5. They shall notify their risk-preparedness plans to the Commission without delay.

7. The competent authorities and the Commission shall publish the risk-preparedness plans on their websites, while ensuring confidentiality of sensitive information, in particular information on measures relating to the prevention or mitigation of consequences of malicious attacks. The protection of the confidentiality of sensitive information shall be based on the principles determined pursuant to Article 19.

8. The competent authorities shall adopt and publish their first risk-preparedness plans by 5 January 2022. They shall update them every four years thereafter, unless circumstances warrant more frequent updates.

Article 11. Content of risk-preparedness plans as regards national measures

1. The risk-preparedness plan of each Member State shall set out all national measures that are planned or taken to prevent, prepare for and mitigate electricity crises as identified pursuant to Articles 6 and 7. It shall at least:

(a) contain a summary of the electricity crisis scenarios defined for the relevant Member State and region, in accordance with the procedures laid down in Articles 6 and 7;
(b) establish the role and responsibilities of the competent authority and describe which tasks, if any, have been delegated to other bodies;

(c) describe the national measures designed to prevent or prepare for the risks identified pursuant to Articles 6 and 7;

(d) designate a national crisis coordinator and establish its tasks;

(e) establish detailed procedures to be followed in electricity crises, including the corresponding schemes on information flows;

(f) identify the contribution of market-based measures in coping with electricity crises, in particular demand-side and supply-side measures;

(g) identify possible non-market-based measures to be implemented in electricity crises, specifying the triggers, conditions and procedures for their implementation, and indicating how they comply with the requirements laid down in Article 16 and with regional and bilateral measures;

(h) provide a framework for manual load shedding, stipulating the circumstances in which loads are to be shed and, with regard to public safety and personal security, specifying which categories of electricity users are, in accordance with national law, entitled to receive special protection against disconnection, justifying the need for such protection, and specifying how the

transmission system operators and distribution system operators of the Member States concerned are to decrease consumption;

(i) describe the mechanisms used to inform the public about electricity crises;

(j) describe the national measures necessary to implement and enforce the regional and, where applicable, bilateral measures agreed pursuant to Article 12;

(k) include information on related and necessary plans for developing the future grid that will help to cope with the consequences of identified electricity crisis scenarios.

2. National measures shall take full account of the regional and, where applicable, bilateral measures agreed pursuant to Article 12 and shall endanger neither the operational security or safety of the transmission system, nor the security of electricity supply of other Member States.

Article 12. Content of risk-preparedness plans as regards regional and bilateral measures

1. In addition to the national measures referred to in Article 11, the risk-preparedness plan of each Member State shall include regional and, where applicable, bilateral measures to ensure that electricity crises with a cross-border impact are properly prevented or managed. Regional measures shall be agreed within the region concerned between Member States that have the technical ability to provide each other assistance in accordance with Article 15. For that purpose, Member States may also form subgroups within a region. Bilateral measures shall be agreed between Member States which are directly connected but are not within the same region. Member States shall ensure consistency between regional and bilateral measures. Regional and bilateral measures shall include at least:

(a) the designation of a crisis coordinator;

(b) mechanisms to share information and cooperate;

(c) coordinated measures to mitigate the impact of an electricity crisis, including a simultaneous electricity crisis, for the purpose of assistance in accordance with Article 15;

(d) procedures for carrying out annual or biennial tests of the risk-preparedness plans;

(e) the trigger mechanisms of non-market-based measures that are to be activated in accordance with Article 16(2).

2. The Member States concerned shall agree the regional and bilateral measures to be included in the risk- preparedness plan after consulting the relevant regional coordination centres. The Commission may have a facilitating role in the preparation of the agreement on regional and bilateral measures. The Commission may request ACER and the ENTSO for Electricity to provide technical assistance to Member States with a view to facilitating such an agreement. At least eight months before the deadline for the adoption or the updating of the risk-preparedness plan, the competent authorities shall report on the agreements reached to the ECG. If the Member States are not able to reach an agreement, the competent authorities concerned shall inform the Commission of the reasons for such disagreement. In such a case the Commission shall propose measures including a cooperation mechanism for the conclusion of an agreement on regional and bilateral measures.

3. With the involvement of relevant stakeholders, the competent authorities of the Member States of each region shall periodically test the effectiveness of the procedures developed in risk-preparedness plans for preventing electricity crises, including the mechanisms referred to in point (b) of paragraph 1, and carry out biennial simulations of electricity crises, in particular testing those mechanisms.

Article 13. Commission assessment of the risk-preparedness plans

1. Within four months of the notification of the adopted risk-preparedness plan by the competent authority, the Commission shall assess the plan taking duly into account the views expressed by the ECG.

2. The Commission shall, after consulting the ECG, issue a non-binding opinion, setting out detailed reasons, and submit it to the competent authority, with a recommendation to review its risk-preparedness plan where that plan:

(a) is not effective to mitigate the risks identified in the electricity crisis scenarios;

(b) is inconsistent with the electricity crisis scenarios identified or with the risk-preparedness plan of another Member State;

(c) does not comply with the requirements laid down in Article 10(2);

(d) sets out measures that are likely to jeopardise the security of electricity supply of other Member States;

(e) unduly distorts competition or the effective functioning of the internal market; or

(f) does not comply with the provisions of this Regulation or other provisions of Union law.

3. Within three months of receipt of the Commission's opinion referred to in paragraph 2, the competent authority concerned shall take full account of the Commission's recommendation and shall either notify the amended risk-preparedness plan to the Commission or notify the Commission of the reasons why it objects to the recommendation.

4. In the event that the competent authority objects to the Commission's recommendation, the Commission may, within four months of receipt of the notification of the competent authority's reasons for objection, withdraw its recommendation or convene a meeting with the competent authority and, where the Commission considers it to be necessary, the ECG, in order to assess the issue. The Commission shall set out detailed reasons for requesting any modifications to the risk-preparedness plan. Where the final position of the competent authority concerned diverges from the Commission's detailed reasons, that competent authority shall provide the Commission with the reasons for its position within two months of receipt of the Commission's detailed reasons.

CHAPTER IV

Managing electricity crises

Article 14. Early warning and declaration of an electricity crisis

1. Where a seasonal adequacy assessment or other qualified source provides concrete, serious and reliable information that an electricity crisis may occur in a Member State, the competent authority of that Member State shall, without undue delay, issue an early warning to the Commission, the competent authorities of the Member States within the same region and, where they are not in the same region, the competent authorities of the directly connected Member States. The competent authority concerned shall also provide information on the causes of the possible electricity crisis, on measures planned or taken to prevent an electricity crisis and on the possible need for assistance from other Member States. The information shall include the possible impacts of the measures on the internal electricity market. The Commission shall provide that information to the ECG.

2. When confronted with an electricity crisis, the competent authority shall, after consulting the transmission system operator concerned, declare an electricity crisis and inform the competent authorities of the Member States within the same region and, where they are not in the same region, the competent authorities of directly connected Member States, as well as the Commission,

without undue delay. That information shall include the causes of the deterioration of the electricity supply situation, the reasons for declaring an electricity crisis, the measures planned or taken to mitigate it and the need for any assistance from other Member States.

3. Where they consider the information provided pursuant to paragraph 1 or 2 to be insufficient, the Commission, the ECG or the competent authorities of the Member States within the same region and, where they are not in the same region, the competent authorities of directly connected Member States may request the Member State concerned to provide additional information.

4. Where a competent authority issues an early warning or declares an electricity crisis, the measures set out in the risk-preparedness plan shall be followed to the fullest extent possible.

Article 15. Cooperation and assistance

Member States shall act and cooperate in a spirit of solidarity in order to prevent or manage electricity crises.

Where they have the necessary technical ability, Member States shall offer each other assistance by means of regional or bilateral measures that have been agreed pursuant to this Article and to Article 12 before that assistance is provided. To that end, and with the purpose of protecting public safety and personal security, Member States shall agree on regional or bilateral measures of their choice in order to deliver electricity in a coordinated manner.

3. Member States shall agree on the necessary technical, legal and financial arrangements for the implementation of the regional or bilateral measures before assistance is offered. Such arrangements shall specify, inter alia, the maximum quantity of electricity to be delivered at regional or bilateral level, the trigger for any assistance and for suspension of assistance, how the electricity will be delivered, and provisions on fair compensation between Member States in accordance with paragraphs 4, 5 and 6.

4. Assistance shall be subject to a prior agreement between the Member States concerned with regard to fair compensation, which shall cover at least:

(a) the cost of the electricity delivered into the territory of the Member State requesting assistance as well as the associated transmission costs; and

(b) any other reasonable costs incurred by the Member State providing assistance, including as regards reimbursement for assistance prepared without effective activation, as well as any costs resulting from judicial proceedings, arbitration proceedings or similar proceedings and settlements.

5. Fair compensation pursuant to paragraph 4 shall include, inter alia, all reasonable costs that the Member State providing assistance incurs from an obligation to pay compensation by virtue of fundamental rights guaranteed by Union law and by virtue of the applicable international obligations when implementing the provisions of this Regulation on assistance and further reasonable costs incurred from the payment of compensation pursuant to national compensation rules.

6. The Member State requesting assistance shall promptly pay, or ensure the prompt payment of fair compensation to the Member State providing assistance.

7. The Commission shall, by 5 January 2020, after consulting the ECG and ACER, provide for non-binding guidance on the key elements of the fair compensation referred to in paragraphs 3 to 6 and other key elements of the technical, legal and financial arrangements referred to in paragraph 3 as well as on general principles of mutual assistance referred to in paragraph 2.

8. In the event of an electricity crisis in which Member States have not yet agreed on regional or bilateral measures and technical, legal and financial arrangements pursuant to this Article, Member States shall agree on ad hoc measures and arrangements in order to apply this Article,

including as regards fair compensation pursuant to paragraphs 4, 5 and 6. Where a Member State requests assistance before such ad hoc measures and arrangements have been agreed, it shall undertake, prior to receiving assistance, to pay fair compensation in accordance with paragraphs 4, 5 and 6.

9. Member States shall ensure that the provisions of this Regulation on assistance are implemented in accordance with the Treaties, the Charter of Fundamental Rights of the European Union and other applicable international obligations. They shall take the necessary measures to that end.

Article 16. Compliance with market rules

1. Measures taken to prevent or mitigate electricity crises shall comply with the rules governing the internal electricity market and system operation.

2. Non-market-based measures shall be activated in an electricity crisis only as a last resort if all options provided by the market have been exhausted or where it is evident that market-based measures alone are not sufficient to prevent a further deterioration of the electricity supply situation. Non-market-based measures shall not unduly distort competition and the effective functioning of the internal electricity market. They shall be necessary, proportionate, non-discriminatory and temporary. The competent authority shall inform relevant stakeholders in its Member State of the application of any non-market-based measures.

3. Transaction curtailment including curtailment of already allocated cross zonal capacity, limitation of provision of cross zonal capacity for capacity allocation or limitation of provision of schedules shall be initiated only in accordance with Article 16(2) of Regulation (EU) 2019/943, and the rules adopted to implement that provision.

CHAPTER V

Evaluation and monitoring

Article 17. Ex post evaluation

1. As soon as possible and in any event three months after the end of an electricity crisis, the competent authority of the Member State that declared the electricity crisis shall provide the ECG and the Commission with an *ex post* evaluation report, after having consulted the regulatory authority, where the regulatory authority is not the competent authority.

2. The ex post evaluation report shall include at least:

(a) a description of the event that triggered the electricity crisis;

(b) a description of any preventive, preparatory and mitigating measures taken and an assessment of their proportionality and effectiveness;

(c) an assessment of the cross-border impact of the measures taken;

(d) an account of the assistance prepared, with or without effective activation, provided to or received from neighbouring Member States and third countries;

(e) the economic impact of the electricity crisis and the impact of the measures taken on the electricity sector to an extent allowed by data available at the time of the assessment, in particular the volumes of energy non-served and the level of manual demand disconnection (including a comparison between the level of voluntary and forced demand disconnection);

(f) reasons justifying the application of any non-market-based measures;

(g) any possible improvements or proposed improvements to the risk-preparedness plan;

(h) an overview of possible improvements to grid development in cases where insufficient network development caused or contributed to the electricity crisis.

3. Where they consider the information provided in the ex post evaluation report to be insufficient, the ECG and the Commission may request the competent authority concerned to provide additional information.

4. The competent authority concerned shall present the results of the ex post evaluation at a meeting of the ECG. Those results shall be reflected in the updated risk-preparedness plan.

Article 18. Monitoring

1. In addition to carrying out other tasks set out in this Regulation, the ECG shall discuss:

(a) the results of the 10-year network development plan in electricity prepared by the ENTSO for Electricity;

(b) the coherence of the risk-preparedness plans, adopted by the competent authorities following the procedure referred to in Article 10;

(c) the results of the European resource adequacy assessments carried out by the ENTSO for Electricity as referred to in Article 23(4) of Regulation (EU) 2019/943;

(d) the performance of Member States in the area of security of electricity supply taking into account at least the indicators calculated in the European resource adequacy assessment, namely the expected energy non-served and loss of load expectation;

(e) the results of the seasonal adequacy assessments referred to in Article 9(2);

(f) the information received from the Member States pursuant to Article 7(4);

(g) the results of the ex post evaluation referred to in Article 17(4);

(h) the methodology for short-term adequacy assessment referred to in Article 8;

(i) the methodology for identifying regional electricity crisis scenarios referred to in Article 5.

2. The ECG may issue recommendations to the Member States as well as to the ENTSO for Electricity related to the matters referred to in paragraph 1.

3. ACER shall, on an ongoing basis, monitor the security of electricity supply measures and shall report regularly to the ECG.

4. By 1 September 2025, the Commission shall, on the basis of the experience gained in the application of this Regulation, evaluate the possible means by which to enhance security of electricity supply at Union level and submit a report to the European Parliament and to the Council on the application of this Regulation, including, where necessary, legislative proposals to amend this Regulation.

Article 19. Treatment of confidential information

1. Member States and competent authorities shall implement the procedures referred to in this Regulation in accordance with the applicable rules, including national rules relating to the handling of confidential information and processes. If the implementation of those rules results in information not being disclosed, inter alia as part of risk-preparedness plans, the Member State or authority may provide a non-confidential summary thereof, and shall do so upon request.

2. The Commission, ACER, the ECG, the ENTSO for Electricity, Member States, competent authorities, regulatory authorities and other relevant bodies, entities or persons, which receive confidential information pursuant to this Regulation, shall ensure the confidentiality of sensitive information.

CHAPTER VI

Final provisions

Article 20. Cooperation with the Energy Community Contracting Parties
Where the Member States and the Energy Community Contracting Parties cooperate in the area of security of electricity supply, such cooperation may include defining an electricity crisis, the process of the identification of electricity crisis scenarios and the establishment of risk-preparedness plans so that no measures are taken that endanger the security of electricity supply of the Member States, Energy Community Contracting Parties or the Union. In that respect, the Energy Community Contracting Parties may, at the invitation of the Commission, participate in the ECG with regard to all matters with which they are concerned.

Article 21. Derogation
Until Cyprus is directly connected with another Member State, Articles 6 and 12 and Article 15(2) to (9) shall not apply either between Cyprus and other Member States, or to the ENTSO for Electricity as regards Cyprus. Cyprus and relevant other Member States may develop, with the support of the Commission, measures and procedures alternative to those provided for in Articles 6 and 12 and Article 15(2) to (9), provided that such alternative measures and procedures do not affect the effective application of this Regulation between the other Member States.

Article 22. Transitional provision pending the establishment of regional coordination centres
Until the date on which regional coordination centres are established pursuant to Article 35 of Regulation (EU) 2019/943, regions shall refer either to a Member State or to a group of Member States located in the same synchronous area.

Article 23. Repeal
Directive 2005/89/EC is repealed.

(…)

ANNEX

TEMPLATE FOR RISK-PREPAREDNESS PLAN

The following template shall be completed in English.

General information

- Name of the competent authority responsible for the preparation of this plan

- Member States in the region

1. SUMMARY OF THE ELECTRICITY CRISIS SCENARIOS

Describe briefly the electricity crisis scenarios identified at regional and national level in accordance with the procedure laid down in Articles 6 and 7, including the description of the assumptions applied.

2. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY

Define the role and responsibilities of the competent authority and the bodies to which tasks have been delegated. Describe which tasks, if any, have been delegated to other bodies.

3. PROCEDURES AND MEASURES IN THE ELECTRICITY CRISIS

3.1. National procedures and measures

(a) Describe procedures to be followed in the cases of an electricity crisis, including the corresponding schemes on information flows;

(b) Describe preventive and preparatory measures;

(c) Describe measures to mitigate electricity crises, in particular demand-side and supply-side measures, whilst indicating in which circumstances such measures can be used especially the trigger of each measure. Where non-market-based measures are considered, they must be duly justified in light of the requirements laid down in Article 16 and must comply with regional and, where applicable, bilateral measures;

(d) Provide a framework for manual load shedding, stipulating under which circumstances loads are to be shed. Specify with regard to public safety and personal security which categories of electricity users are entitled to receive special protection against disconnection, and justify the need for such protection. Specify how the transmission system operators and the distribution system operators should act in order to decrease the consumption;

(e) Describe the mechanisms used to inform the public about the electricity crisis.

3.2. Regional and bilateral procedures and measures

(a) Describe the agreed mechanisms for cooperation within the region and for ensuring appropriate coordination before and during the electricity crisis, including the decision-making procedures for appropriate reaction at regional level;

(b) Describe any regional and bilateral measures that have been agreed, including any necessary technical, legal and financial arrangements for the implementation of those measures. When describing such arrangements, provide information on, inter alia, the maximum quantities of electricity to be delivered at regional or bilateral level, the trigger for the assistance and possibility to request its suspension, how the electricity will be delivered, and the provisions on fair compensation between Member States. Describe the national measures necessary to implement and enforce the regional and bilateral measures agreed;

(c) Describe the mechanisms in place for cooperation and for coordinating actions, before and during the electricity crisis, with other Member States outside of the region as well as with third countries within the relevant synchronous area.

4. CRISIS COORDINATOR

Indicate and define the role of the crisis coordinator. Specify the contact details.

5. STAKEHOLDER CONSULTATIONS

In accordance with Article 10(1), describe the mechanism used for and the results of the consultations carried out, for the development of this plan, with:

(a) relevant electricity and natural gas undertakings, including relevant producers or their trade bodies;

(b) relevant organisations representing the interests of non-industrial electricity customers;

(c) relevant organisations representing the interests of industrial electricity customers;

(d) regulatory authorities;

(e) the transmission system operators;

(f) relevant distribution system operators.

6. EMERGENCY TESTS

(a) Indicate the calendar for the biennial regional (and, if applicable also national) real time response simulations of electricity crises;

(b) In accordance with point (d) of Article 12(1), indicate procedures agreed and the actors involved.

For the updates of the plan: briefly describe the tests carried out since the last plan was adopted and the main results. Indicate which measures have been adopted as a result of those tests.

See also:

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC

Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003

Regulation (EU) No 347/2013 of the European Parliament and of the Council of 17 April 2013 on guidelines for trans-European energy infrastructure and repealing Decision No 1364/2006/EC and amending Regulations (EC) No 713/2009, (EC) No 714/2009 and (EC) No 715/2009

Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation

Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration

Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators (recast)

Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast)

ENISA Publications

1.33 Power Supply Dependencies in the Electronic Communications Sector: Survey, analysis and recommendations for resilience against power supply failures (2013)

Executive summary

Electronic communications are the backbone of the EU's digital society. The electronic communications networks and services allow citizens, businesses, governments and organisations to communicate and exchange information and to offer and consume online

services. Article 13a of the EU's electronic communications Framework directive, which was implemented across the EU in 2011, asks EU Member States to ensure the security and resilience of public electronic communications networks and services.

As part of the implementation of Article 13a, National Regulatory Authorities (NRAs) in the EU collect reports about incidents with a significant impact on the electronic communications networks and services. Yearly, ENISA publishes an annual report which summarizes these incident reports and provides an aggregate analysis of major outages. As can be seen in the ENISA annual report about major incidents, power cuts are a dominant cause of severe network and service outages in the EU's electronic communications sector.

In this report, we study these incidents in more detail and we make recommendations to NRAs and electronic communications service providers (providers) and to some extent also to actors in the energy sector as well as civil protection authorities. Our recommendations are not about preventing power failures in the power supply sector, but they are aimed at improving the electronic communications sector's ability to withstand and act efficiently after power cuts.

ENISA conducted an online survey and interviews about how power cuts are handled in the electronic communications sector. We found that:

- A majority of EU Member States have implemented more general resilience policies through legislation, whereas a minority of the Member States have implemented policies that are directly linked to resilience against power cuts.

- A majority of the NRAs do not and may even lack suitable input to perform risk assessments that include power cuts. It is also noted that the national use of state funding and public- private partnerships to address power cut resilience are exceptions rather than the norm within the EU.
- Resilience against power cuts is lower in access networks closer to customers than for network elements that carry traffic for a large number of customers. Mobile networks tend to be more vulnerable to power cuts compared to fixed networks.

- A majority of NRAs believe that current protection levels are not adequate and they would like to see power cut resilience to become a market differentiating factor for network and providers.
- A review of incident reports from 2011 and 2012 shows that a significant number of power cuts led to more severe service disruptions than what would have been the case had existing protection measures worked as intended.

- A large number of energy sector regulators within Europe have adopted regulatory instruments to maintain or improve continuity of supply in the energy sector, balancing other regulations aiming at increasing competition and market efficiency.

- In some countries, the energy sector has taken significant steps in defining socio- economically acceptable quality of service levels, whereas in some countries the providers face the fact that there are no special contractual agreements with the power companies containing SLA-based requirements.
- Cooperation and information exchange can be improved within the electronic communications sector and with the energy sector and civil protection authorities, and the room for improvement is even more significant for cross-sector restoration efforts.

- Prioritization schemes to give assets within the electronic communications sector preferential treatment in the event of more significant power cuts, are not yet widespread in the EU.

We also make 8 recommendations mainly to NRAs and providers within the electronic communications sector, and in some recommendations we also address the energy sector and civil protection authorities. The recommendations describe steps which could be taken to reduce the risk of network and service outages caused by power failures, and in this way improve the electronic communications sector's ability to handle disruptions and outages caused by power supply failures. Summarizing the recommendations:

1. NRAs should analyse the frequency and impact of network and service outages caused by power cuts.

2. NRAs should liaise with providers, energy regulators and other NRAs to collect good practices that could be used to increase resilience against power cuts. These good practices should be considered as part of a cost-benefit analysis (recommendation 3).

3. NRAs should perform, in cooperation with energy regulators and civil protection authorities, a cost-benefit analysis, where societal costs and benefits are evaluated, to determine what is reasonable to expect from different actors regarding power cut resilience measures.

4. Providers should regularly perform checks of existing protection measures, such as checks of UPS systems and batteries, and running facilities with fixed and transportable power generators at full load, to avoid and mitigate the impact of network and service outages from shorter and medium duration power cuts.

5. NRAs should in their follow up of major network and service outages caused by power cuts ensure that affected providers, based on lessons learned, systematically develop their protection measures to avoid and mitigate the impact of network and service outages from shorter and medium duration power cuts.

6. NRAs should act to establish a strategy to promote cooperation and mutual aid agreements on joint service restoration after severe power cuts which can include cross-sector exercises.

7. NRAs should consider a priority scheme that would give preferential treatment within the electronic communications sector and decrease service restoration times under exceptional circumstances.

8. NRAs, providers, actors in the energy sector, civil protection authorities and other societal functions should cooperate to establish information exchange mechanisms. These mechanisms should enable an efficient exchange of situational awareness information, forecasts of restoration times and other information that is essential for the efficient restoration after severe power cuts.

More details can be found in the body of this report. We look forward to working with the NRAs and providers to mitigate the impact of network and security incidents caused by power supply failures. We encourage the different actors to find ways to improve information-sharing about failures and outages, particularly between the energy sector and the electronic communications sector.

(…)

1.34 Smart Grid Security: Recommendations for Europe and Member States (2012)

Executive Summary

The smart grid can be defined as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added. Smart grids will be able to efficiently integrate the behaviour and actions of all users connected to them - generators, consumers and those that do both - in order to ensure an economically efficient, sustainable power system with low losses and high quality and security of supply and safety.

Information and Communication Technologies (ICT) are envisioned to be the underpinning platform of smart grids, which exemplifies the increasing dependency of the European economy and society on communication networks and computer applications. Smart grids give clear advantages and benefits to the whole society, but their dependency on computer networks and applications, as well as on the Internet, makes our society more vulnerable to malicious cyber attacks with potentially devastating results.

Recognising the importance of the problem, ENISA launched a series of activities, which include the present study, aiming at bringing together the relevant stakeholders and engaging them in an open discussion on smart grid cyber security. The principal goal of the open dialogue is to identify the main concerns regarding the security of smart grids as well as to recognize and support national, pan-European and international initiatives on smart grid security.

This study makes 10 recommendations to the public and private sector involved in the definition and implementation of smart grids. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, raising awareness, developing new measures and good practices, and reducing barriers to information sharing. This guidance is based on the results of a thorough analysis of the opinions of the experts who participated in the study. Furthermore, important information coming from in-depth desktop research is also taken into consideration. All this data has been analysed and has provided almost 100 Key Findings.

The top ones are:

Recommendation 1. The European Commission (EC) and the Member States '(MS) competent authorities should undertake initiatives to improve the regulatory and policy framework on smart grid cyber security at national and EU level.

Recommendation 2. The EC in cooperation with ENISA and the MS should promote the creation of a Public-Private Partnership (PPP) to coordinate smart grid cyber security initiatives.

Recommendation 3. ENISA and the EC should foster awareness raising and training initiatives.

Recommendation 4. The EC and the MS in cooperation with ENISA should foster dissemination and knowledge sharing initiatives.

Recommendation 5: The EC, in collaboration with ENISA and the MS and the private sector, should develop a minimum set of security measures based on existing standards and guidelines.

Recommendation 6. Both the EC and the MS competent authorities should promote the development of security certification schemes for components, products and organisational security.

Recommendation 7. The EC and MS competent authorities should foster the creation of test beds and security assessments.

Recommendation 8: The EC and the MS, in cooperation with ENISA, should further study and refine strategies to coordinate measures countering large scale pan-European cyber incidents affecting power grids.

Recommendation 9: The MS competent authorities in cooperation with CERTs should initiate activities in order to involve CERTs to play an advisory role in dealing with cyber security issues affecting power grids.

Recommendation 10. EC and the MS competent authorities in cooperation with the Academia and the R&D sector should foster research in smart grid cyber security, leveraging existing research programmes (…)

1.35 Appropriate security measures for smart grids: Guidelines to assess the sophistication of security measures implementation (2012)

Preface

The development of an efficient, reliable and sustainable environment for the production and distribution of energy in the future is linked to the use of smart grids. Various market drivers,

regulatory or standardisation initiatives have appeared or gained importance as tools to help involved stakeholders to be prepared against smart grids security vulnerabilities and attacks. The perception and the approach taken on this topic differ among stakeholders. This underlines the importance of the stakeholder's alignment on the key aspects related to the smart grid security.

The European Network and Information Security Agency (ENISA) has decided to further investigate the challenges of ensuring an adequate smart grid protection in Europe, in order to help smart grid providers to improve the security and the resilience of their infrastructures and services. Defining a common approach to addressing smart grid cyber security measures will help achieve this.

This technical document provides guidance to smart grid stakeholders by providing a set of minimum security measures which might help in improving the minimum level of their cyber security services. The proposed security measures are organised into three (3) sophistication levels and ten (10) domains, namely:

1. Security governance & risk management;
2. Management of third parties;
3. Secure lifecycle process for smart grid components/systems and operating procedures;
4. Personnel security, awareness and training;
5. Incident response & information knowledge sharing;
6. Audit and accountability;
7. Continuity of operations;
8. Physical security;
9. Information systems security; and
10. Network security.

The adoption of a particular set of security measures needs the consensus and cooperation of various stakeholders in the smart grid community. A coordination initiative could allow a common and generally accepted approach to addressing smart grid security issues. Moreover, the development of a common approach to addressing smart grid cyber security measures will help not only regulators by harmonising the complex smart grid's environment but also by providing incentives to other involved stakeholders to continuously strive for the improvement of their cyber security.

(…)

1.36 Smart Grid Threat Landscape and Good Practice Guide (2013)

Executive summary

Smart grids are complex systems. A smart grid is a system of systems delivering energy to consumers. Smart grid stores, transports and manages energy. Smart grid is a *de facto* Critical Infrastructure as energy is important for the well-functioning of the society and economy. Being the blending of the energy and telecommunication critical infrastructures, smart grids should operate securely and by respecting end users 'privacy. Moreover, the protection of the smart grid is the key to energy availability. In this document we elaborate on cyber security issues with regards to smart grid information infrastructure.

The security of a complex system is also a complex matter. In order to cope with this complex environment, this document leverages the following principles for simplifying the problem:

Consider external and internal threats: In cyber-security the external environment are the cyber-threats. This cyber-threat environment originates from threat agents, the adversaries utilizing cyber-threats and launching cyber-attacks. Although dynamically changing, the cyber-threat

landscape can be described and has finite elements. An understanding of the cyber-threat landscape is indispensable for the identification of the necessary protection measures. In this document, we provide a threat landscape affecting smart grid components. Internal threats are considered as well: a variety of threats emanating from errors and insider attacks are also taken into account.

Decompose and classify the elements: A decomposition of smart grid components is one of the main tasks to tackle its complexity. This task is currently being performed by various experts around Europe and the World. Within this report, we have adopted the smart grid decomposition provided in the document Smart Grid Reference Architecture of the Smart Grid Standardization Coordination Group of CEN-CENELEC-ETSI. This is because this work is a highly reputed document among the security experts in Europe.

Capture available knowledge: What have others done in the area of smart grid protection? This has been addressed by taking stock of available cyber-security approaches, protection approaches and good practices developed recently.

In response to the urgent question of many stakeholders: How does this document support me in my work? this document provides tools to assess risk exposure of smart grid assets and will show what others have done in this respect. It elaborates on the threats smart grid components are exposed to and on the security controls to reduce threat exposure. But the assessment on the living object can be done only by the asset owner, just because asset owners master the complexity of infrastructures and the interdependencies among various assets. This task cannot be done as a generic exercise or it would have low value.

Concluding, one should note that the use of these tools will depend on the capabilities of the expert users. In cyber-security preparedness, however, much depends on the capabilities of the adversary, which are not always known and certain;

“That which depends on me, I can do; that which depends on the enemy cannot be certain. Therefore it is said that one may know how to win, but cannot necessarily do so” (Sun Tzu).

Being knowledgeable about what can be achieved is one thing. The other is to reduce the impact. In cyber-security - an environment with asymmetric approaches - this can be achieved through common effort and coordination.

(…)

1.37 Smart grid security certification in Europe: Challenges and recommendations (2014)

Executive summary

Security and privacy issues are of major concern for smart grid users. For this reason, vendors should ensure that these two features follow smart grid devices for their whole life cycle; from the design to the decommission phase. Certification is not only a means to provide assurance to the smart gird users that security and privacy have been taken into account but also to create trust to the entire smart grid supply chain.

This report provides insight on security certification of smart grids. It contains information about several certification approaches; it describes the specific European situation, discusses the advantages and challenges and provides recommendations to involved stakeholders towards a more harmonised European smart grid security certification practices framework.

The report describes the need for harmonised European smart grid certification practices which cover the complete smart grid supply chain, and are supported by a European platform based on M/490 SGAM (Smart Grid Architecture Model) and the concept of smart grid chain of trust. Part of this report is the analysis of the available security certification schemes for smart grids and the

approaches used in Europe. This way we have generated an overview that depicts which certification schemes can be used to create this chain of trust. During this analysis it came up that there is not a single, existing, scheme that can cover the entire chain of trust, and that not all parts of the chain can be completely covered for every smart grid use-case. Additionally, it appeared that there are multiple initiatives in different Member States that take different approaches to achieve the same goal. For this reason, we use the common denominator of the features of the different existing certification standards in order to introduce a certification meta-scheme for the smart grids in Europe.

The major gaps and challenges of a European smart grid certification scheme revolve around the fragmentation and different approaches in Member States, as well as the lack of EU guidance by a trusted oversight body. At this moment it will be difficult to create a security certification scheme that completely confronts the identified challenges, but an approach can be outlined that describes how to go from the current fragmented situation to a more harmonised one at the EU level. This approach allows for the national specific approaches and requirements, while providing possibilities to adopt European based requirements to facilitate harmonisation, and benefit from joined standardisation efforts.

Taking into account the needs, as expressed in various referenced resources, we also outline the properties of the ‘ideal ’smart gird cyber security apparatus. To achieve this ‘ideal ’situation a set of recommendations is addressed to the main stakeholders; the Commission, the certification bodies, the Member States and the private sector. The most outstanding recommendations are:

Harmonised EU smart grid security certification practices

More harmonised and coordinated EU smart grid certification practices will act as an umbrella and should contain elementary properties that national schemes need to have. European accreditation bodies will be used for confirmation of national schemes. This will ensure that there is not a single certifying authority, and the process remains impartial. Next to this, private sector will help in keeping up with the latest technology specific requirements and guidance consolidated by technical committees. The committees should amend the slow moving standards with detailed protection profiles or security requirements. Updates in national schemes should be announced so that they can be incorporated in national profiles. This way the maturity of the national schemes can evolve over time.

The Commission together with the Member States should promote certification by allowing for commercial advantages for the private sector when following practices which lead to more harmonisation across Europe (e.g. criteria for E.U procurement activities). The certification practices should provide European guidance, facilitate national legislation and be actively promoted as a means for more harmonization.

National implementation of specific smart grid use cases based on a chain of trust

Each Member State should be able to map its preferred national standard/scheme to the EU platform and refer to this national standard for details. They should also be able to amend or expand on the European security requirements to provide the flexibility to incorporate national specific requirements. The national profiles should be created by national groups, but could be based on the published schemes of other Member States. The national profiles can contain the national specific technical requirements regarding the needed security features related to the applicable use cases used in that Member State. Additionally they should contain test procedures for the national specific requirements, and define the required testing levels for the national use cases aligned with the international SG-IS2 framework risk levels.

Oversight

It is recommended to create a EU steering committee with oversight competences on smart grid certification, the definition of pan European security requirements ’and the development of

national schemes. It should be responsible for centralised storage and the publication of smart grid certificates and adopted schemes, to facilitate clarity on what is certified and how. It should provide implementation guidance and recommendations based on the most recent best practices and informative standards.

The EU steering committee will have only a coordination role and act as an advisor to the certification bodies, making sure the latest threats are reflected in the security requirements definition process.

To this end, this committee will take feedback from the private sector, and lessons learned during the certification processes of other nationalities.

The steering committee should create and maintain a landing page with specific explanations for all stakeholders about smart grid security certification concepts, their place in the chain of trust and how to implement a smart grid certification chain of trust on a specific smart grid use case.

(…)

1.38 Communication network interdependencies in smart grids (2015)

Smart grids can be described as a new generation of smart power networks that integrate actions coming from all connected end-users. This infrastructure provides bidirectional communications between end-users and the grid operator, and therefore extends the attack surface against the power system.

However, one point that has been constantly overlooked and has not received the attention it deserves concerns the interdependencies and communications between all the assets that make up the new power grids. These interdependencies in communications are a fundamental pillar, as they represent the means by which all devices communicate within the smart grid network.

Information transmitted through these intercommunications contains not only customer and consumption data; but also status checks, instructions to execute, orders for devices to redirect power flow, etc. Therefore, their protection is essential to protect the privacy of the customers and prevent attacks which could cause blackouts, power overloads, device malfunctions, data tampering, or even catastrophic cascading effects that could bring down the power grid itself in more than one country.

For this purpose, this study focuses on the evaluation of these interdependencies, and their architectures and connections in order to determine their importance, threats, risks, mitigation factors and possible security measures to implement. To obtain this information, experts in the fields and areas related directly with smart grids were contacted to gather their know-how and expertise.

The concerns that were expressed by these experts can be sorted into two main categories, technical recommendations and organizational recommendations:

- Regarding smart grid devices, these devices are now exposed to different networks, and therefore their periodic update becomes essential in order to ensure that they are protected against the latest threats that appear. Furthermore, these devices should also implement by default security measures to protect them (such as authentication, encryption or frame counters), as implementing such measures in the deployment phase is much more costly and does not reach the same level of security.

- Regarding the communications interdependencies, the main concern is with the protocols used on the smart grids. There is an urgent need to harmonize the current situation by establishing common interconnection protocols to be used by all devices, and ensure that these protocols implement by default enough security measures to protect the data whilst it is in transit (such as encryption or mutual authentication).

- Finally there is the need to align policies, standards and regulations across EU Member States to ensure the overall security of smart grids. This is now even more important due to the risk that cascading failures can cause; as smart grid communication networks are no longer limited by physical or geographical barriers, and an attack on one country could translate into another.

Additionally, due to the global and distributed nature of many of these threats, it becomes necessary for European organizations, distributors, utilities and the rest of involved stakeholders to share knowledge on these attacks both on incident management and incident reporting level.

In conclusion, the protection of the intercommunications in smart grid networks is essential in order to ensure the correct operation of the network and the protection of private and sensitive data. Furthermore, it is necessary in order to protect against attacks to the power grid, therefore making it a matter of national and European interest. For this purpose, the following recommendations have been developed:

Recommendation 1: European Commission should ensure the alignment of policy approaches across EU countries to establish a common posture for smart grid communication interdependencies. Cyber security has become one of the main concerns regarding the implementation of smart grids, and especially concerning the networks used for the interconnection of all the assets that make up this new grid. Therefore, it is inherently necessary to protect these communication networks, the data that is transmitted through them and the devices connected to them. European Commission should ensure the alignment of the requirements and standards for smart grid communication networks, especially regarding the homologation of security devices and protocols.

Recommendation 2: Manufacturers and vendors should foster intercommunication protocol compatibility between devices from different manufacturers and vendors. Currently, many manufacturers and vendors, due to the lack of standards, make use of their own proprietary protocols and communication systems for the intercommunication between their devices. Therefore, when a distributor or utility makes use of these devices, the rest of the network devices have to be provided by the same vendor, or have to be specifically compatible with them. Distributors, utilities and other actors involved should make use of devices acquired from various supply lines without having to be concerned about incompatibilities in the communication among them.

Recommendation 3: European smart grid operators and relevant authorities should develop a set of minimum security requirements to be applied in all communication interdependencies in smart grids. Security controls must be defined to reach a minimum level of security that ensures service connectivity continuity and resilience, both in public and private environments. This could be done by establishing a working group at European level, with representation of all relevant stakeholders, in order to define a series of recommendations regarding the minimum security requirements that should always be applied to smart grid devices, intercommunications and interdependencies.

Recommendation 4: Manufacturers, vendors and asset owners should implement security measures on all devices and protocols that are part, or make use of the smart grid communication network. Traditionally, grid devices and assets were usually isolated, or interconnected through private local networks. However, smart grids bring a new level of interconnection, where devices can be connected to large networks, wireless networks and even the Internet. This leads to the need to protect these communications against eavesdropping and tampering, from the origin and up to the destination. This could be achieved by supporting the implementation of security measures by default on all the protocols used for intercommunication within the smart grid network.

Recommendation 5: Manufacturers, vendors and asset owners should work together on updatable devices and periodic security update support. Nowadays, it is the norm for software

and firmware to receive periodic updates to fix vulnerabilities, add new security features or fixes, and even add new capabilities. This is quite common on personal devices and servers, however it is not the case yet in smart grids. Devices must be designed to be easily updated, both their software and firmware, in order to ensure that they maintain an acceptable security level. Manufacturers and vendors should work together on this topic, as they need to design their devices to be easily updatable, and need to develop an update program to maintain them updated.

Recommendation 6: European Commission, Member States and all relevant smart grid stakeholders should promote incident reporting and attack patterns sharing. With the implementation of smart grids, many new attack vectors and network entry points have appeared as a consequence of their intercommunicated and distributed nature. For this reason, it becomes necessary to share data and attack patterns to help all involved agents protect their assets and develop countermeasures which can, in turn, be shared to protect the overall smart grid network.

Recommendation 7: European Commission, Member States and all relevant smart grid stakeholders should promote increased training and awareness campaigns. One of the gripes that threats smart grids is related to the limited number of qualified professionals; a few of the existing ones lacking adequate training regarding security. This is due to in new scenarios that have appeared on energy grids regarding the new features that come with the implementation of smart grid technologies

Artificial Intelligence: Liability, Digital Content and Autonomous Systems

Veronika Žolnerčíková

Communication Artificial Intelligence for Europe

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe. {COM(2018) 237 final}

1. Introduction – embracing change

Artificial intelligence (AI) is already part of our lives – it is not science fiction. From using a virtual personal assistant to organise our working day, to travelling in a self-driving vehicle, to our phones suggesting songs or restaurants that we might like, AI is a reality.

Beyond making our lives easier, **AI is helping us to solve some of the world's biggest challenges: from treating chronic diseases or reducing fatality rates in traffic accidents**[182] **to fighting climate change or anticipating cybersecurity threats**.

In Denmark, AI is helping save lives by allowing emergency services to diagnose cardiac arrests or other conditions based on the sound of a caller's voice. In Austria, it is helping radiologists detect tumours more accurately by instantly comparing x-rays with a large amount of other medical data.

Many farms across Europe are already using AI to monitor the movement, temperature and feed consumption of their animals. The AI system can then automatically adapt the heating and feeding machinery to help farmers monitor their animals' welfare and to free them up for other tasks. And AI is also helping European manufacturers to become

What is artificial intelligence?

Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.

AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).

We are using AI on a daily basis, e.g. to translate languages, generate subtitles in videos or to block email spam.

Many AI technologies require data to improve their performance. Once they perform well, they can help improve and automate decision making in the same domain. For example, an AI system will be trained and then used to spot cyber-attacks on the basis of data from the concerned network or system.

[182] It is estimated that around 90% of road accidents are caused by human errors. See Commission's report on Saving Lives: Boosting Car Safety in the EU (COM(2016) 0787 final).

more efficient and to help factories return to Europe.[183]

These are some of the many examples of what we know AI can do across all sectors, from energy to education, from financial services to construction. Countless more examples that cannot be imagined today will emerge over the next decade.

Like the steam engine or electricity in the past, AI is transforming our world, our society and our industry[184]. Growth in computing power, availability of data and progress in algorithms have turned AI into one of the **most strategic technologies of the 21st century**. The stakes could not be higher. **The way we approach AI will define the world we live in**. Amid fierce global competition, **a solid European framework is needed**.

The European Union (EU) should have a **coordinated approach** to make the most of the opportunities offered by AI and to address the new challenges that it brings. **The EU can lead the way in developing and using AI for good and for all**, building on its values and its strengths. It can capitalise on:

- **world-class researchers, labs and startups**. The EU is also strong in **robotics** and has **world-leading industry**, notably in the transport, healthcare and manufacturing sectors that should be at the forefront of AI adoption;
- the **Digital Single Market**. Common rules, for example on data protection and the free flow of data in the EU, cybersecurity and connectivity help companies to do business, scale up across borders and encourage investments; and
- a **wealth of industrial, research and public sector data** which can be unlocked to feed AI systems. In parallel to this Communication, the Commission is taking action to make data sharing easier and to **open up more data – the raw material for AI – for re-use**. This includes data from the public sector in particular, such as on public utilities and the environment, as well as research and health data.

European leaders have put AI at the top of their agendas. On 10 April 2018, 24 Member States[185] and Norway committed to working together on AI. Building on this **strong political endorsement**, it is time to make significant efforts to ensure that:

- **Europe is competitive in the AI landscape**, with bold investments that match its economic weight. This is about supporting research and innovation to develop the next generation of AI technologies, and deployment to ensure that companies – in particular small and medium-sized enterprises which make up 99% of business in the EU – are able to adopt AI.
- **No one is left behind in the digital transformation**. AI is changing the nature of work: jobs will be created, others will disappear, most will be transformed. Modernisation of education, at all levels, should be a priority for governments. All Europeans should have every opportunity to acquire the skills they need. Talent should be nurtured, gender balance and diversity encouraged.
- **New technologies are based on values**. The General Data Protection Regulation will become a reality on 25 May 2018. It is a major step for building trust, essential in the long term for both people and companies. This is where the **EU's sustainable approach to technologies** creates a

---

[183] Why AI is the future of growth, Accenture, 2016. The economic impact of the automation of knowledge work, robots and self-driving vehicles could reach between EUR 6.5 and EUR 12 trillion annually by 2025 (including improved productivity and higher quality of life in ageing populations). Source: Disruptive technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute, 2013.

[184] AI is part of the Commission's strategy to digitise industry (COM(2016) 180 final) and a renewed EU Industrial Policy Strategy (COM(2017) 479 final).

[185] Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

competitive edge, by embracing change on the basis of the Union's values[186]. As with any transformative technology, some AI applications may raise new ethical and legal questions, for example related to liability or potentially biased decision-making. The EU must therefore ensure that AI is developed and applied in an appropriate framework which promotes innovation and respects the Union's values and fundamental rights as well as ethical principles such as accountability and transparency. The EU is also well placed to lead this debate on the global stage.

This is how the EU can make a difference – and be the champion of **an approach to AI that benefits people and society as a whole**.

Launching a European initiative on AI

In May 2017, the Commission published its mid-term review of the Digital Single Market strategy[187]. It highlighted the importance of building on Europe's scientific and industrial strengths, as well as on its innovative startups, to be in a leading position in the development of AI technologies, platforms, and applications.

The European Council of October 2017 stated that the EU needs a sense of urgency to address emerging trends such as AI "while at the same time ensuring a high level of data protection, digital rights and ethical standards" and invited "the Commission to put forward a **European approach to artificial intelligence**".[188] The European Parliament made wide-ranging recommendations on civil law rules on robotics and the European Economic and Social Committee has also issued an opinion on the topic.[189]

This Communication sets out a European initiative on AI, which aims to:

- **Boost the EU's technological and industrial capacity and AI uptake across the economy**, both by the private and public sectors[190]. This includes investments in research and innovation and better access to data.
- **Prepare for socio-economic changes** brought about by AI by encouraging the modernisation of education and training systems, nurturing talent, anticipating changes in the labour market, supporting labour market transitions and adaptation of social protection systems.
- **Ensure an appropriate ethical and legal framework**, based on the Union's values and in line with the Charter of Fundamental Rights of the EU. This includes forthcoming guidance on existing product liability rules, a detailed analysis of emerging challenges, and cooperation with stakeholders, through a European AI Alliance, for the development of AI ethics guidelines.[191]

All this requires **joining forces**. Building on the approach set out in this Communication and the declaration[192] of cooperation signed by 24 Member States on 10 April 2018, the Commission will

---

[186] Article 2 of the Treaty on EU: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities". The Member States share a "society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail."

[187] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:228:FIN

[188] http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf

[189] European Parliament resolution with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)); European Economic and Social Committee opinion on AI (INT/806-EESC-2016-05369-00-00-AC-TRA).

[190] AI can significantly improve public services and contribute to the objectives set out in the Ministerial Declaration on eGovernment – the Tallinn Declaration (October 2017, https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration). For example, the Commission will look into AI's potential to analyse large amounts of data and help check how single market rules are applied.

[191] Building on the work of the European Group on Ethics in Science and New Technologies

[192] https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

work with **Member States on a coordinated plan on AI**. The discussion will take place in the framework of the existing European platform of national initiatives to digitise industry, with the view to **agree this plan by the end of 2018**. The main aims will be to maximise the impact of investments at EU and national levels, encourage synergies and cooperation across the EU, exchange best practices and collectively define the way forward to ensure that the EU as a whole can compete globally.

In the coming weeks the Commission will issue a Communication on the future of connected and automated mobility in Europe and a Communication on the future research and innovation ambitions for Europe. AI will be a key element of these initiatives.

2. The EU's position in a competitive international landscape

Most developed economies recognise the game-changing nature of AI and have adopted different approaches which reflect their own political, economic, cultural and social systems.[193]

The government of the United States presented an AI strategy and invested around EUR 970 million in unclassified AI research in 2016. With its 'Next Generation Artificial Intelligence Development Plan', China is targeting global leadership by 2030 and is making massive investments.[194] Other countries, such as Japan and Canada, have also adopted AI strategies.

In the United States and in China, large companies are significantly investing in AI and are exploiting large amounts of data.[195]

Overall, **Europe is behind in private investments** in AI which totalled around EUR 2.4-3.2 billion in 2016, compared with EUR 6.5-9.7 billion in Asia and EUR 12.1-18.6 billion in North America.[196]

It is therefore crucial that the EU continues its work to **create an environment that stimulates investments** and uses public funding to leverage private investments. To do so, the EU needs to **preserve and build on its assets**.

Europe is home to a **world-leading AI research community**, as well as innovative **entrepreneurs** and **deep-tech startups** (founded on scientific discovery or engineering).[197] It has a **strong industry**, producing more than a quarter of the world's industrial and professional service robots (e.g. for precision farming, security, health, logistics)[198], and is leading in manufacturing, healthcare, transport and space technologies – all of which increasingly rely on AI. Europe also plays an important role in the development and exploitation of platforms providing **services to companies and organisations (business-to-business**, applications to progress towards the "intelligent enterprise" and e-government.

One of the main challenges for the EU to be competitive is to **ensure the take-up of AI technology across its economy**. European industry cannot miss the train. Only a fraction of European companies have already adopted digital technologies. This trend is particularly acute in small and

---

[193] See also the Commission's European Political Strategy Centre's Strategic Note: The Age of Artificial Intelligence, 2018.

[194] Recent announcements include a EUR 1.7 billion AI technology park in Beijing.

[195] With 1.4 billion mobile phone subscriptions and 800 million internet users – more than the USA and the EU combined – Chinese people generate vast amounts of personal data that are used to develop related AI products.

[196] 10 imperatives for Europe in the age of AI and automation, McKinsey, 2017.

[197] Europe accounts for the largest share of top 100 AI research institutions worldwide. 32 research institutions in the global top 100 for AI-related research paper citations vs 30 from the USA and 15 from China. Source: Atomico, State of European Tech, 2017. It can also be noted that the German Research Centre for Artificial Intelligence (DFKI) founded in 1988 is one of the world's largest research centres in the field of AI.

[198] World Robotics 2017, International Federation of Robotics. Europe is home to three of the world's largest producers of industrial robots (KUKA, ABB and Comau).

medium-sized businesses. In 2017, 25% of EU large enterprises and 10% of small and medium-sized enterprises used big data analytics. Only one in five small and medium-sized enterprises was highly digitised, while one third of the workforce still does not possess basic digital skills.[199] At the same time, the benefits of adopting AI are widely recognised. For example, the 2018 Digital Transformation Scoreboard shows that businesses in the agrifood and construction sectors which have adopted AI confirm positive impacts on entering new markets, improving products or services, and gaining new clients.[200]

EU efforts so far: laying the groundwork to make the most of AI

AI has featured in the EU research and development framework programmes since 2004 with a specific focus on robotics. Investments increased to up to EUR 700 million for 2014-2020, complemented by EUR 2.1 billion of private investments as part of a public-private partnership on robotics.[201] These efforts have significantly contributed to **Europe's leadership in robotics**.

Overall, around EUR 1.1 billion has been invested in AI-related research and innovation during the period 2014-2017 under the Horizon 2020 research and innovation programme, including in big data, health, rehabilitation, transport and space-oriented research.

***Projects funded by the EU have** developed for example:*

- *an unmanned agricultural vehicle that can mechanically remove weeds, reducing the need for pesticides;*
- *a highway pilot project using AI & Internet of Things to provide safe driving recommendations and reduce road fatalities;*
- *a robotic ortho-prosthesis to restore mobility to amputees;*
- *robots to take care of repetitive tasks for workers in car*

Additionally, the Commission has launched major initiatives which are key for AI. These include the development of more efficient electronic components and systems, such as **chips specifically built to run AI operations** (neuromorphic chips)[202]; **world-class high-performance computers**[203]**,** as well as flagship projects on **quantum technologies** and on the mapping of the **human brain**.[204]

3. The way forward: an EU initiative on AI

3.1. Boosting the EU's technological and industrial capacity and AI uptake across the economy

The public and private sectors must seize the opportunities that come both from developing innovative AI solutions and applying them to a range of fields.[205]

---

[199] https://ec.europa.eu/digital-single-market/digital-scoreboard. According to McKinsey (2016), European companies operating at the digital frontier only reach a digitisation level of 60% compared to their US peers.

[200] https://ec.europa.eu/growth/tools-databases/dem/monitor/scoreboard

[201] https://eu-robotics.net/sparc/.

[202] Neuromorphic chips are modelled on biological structures such as brains. This project is part of the Electronic Components and Systems for European Leadership joint undertaking (EUR 4.8 billion of public-private investments by 2020).

[203] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking. This infrastructure will underpin the European Open Science Cloud that will offer researchers a virtual environment to store, process, share and re-use their data across disciplines and borders: https://ec.europa.eu/research/openscience/

[204] https://ec.europa.eu/digital-single-market/en/fet-flagships

[205] The recent report of the "High Level Group on Industrial Technologies" recognised AI as a "key enabling technology" highlighting the transformative role of AI and the necessity for the industry to use AI to maintain its leadership: http://ec.europa.eu/research/industrial_technologies/pdf/re_finding_industry_022018.pdf

The EU should be **ahead of technological developments in AI** and ensure they are swiftly taken up across its economy. This implies **stepping up investments** to strengthen fundamental research and make scientific breakthroughs, upgrade AI research infrastructure, develop AI applications in key sectors from health to transport, facilitate the uptake of AI and the access to data.
Joint effort by both the public (national and EU levels) **and private sectors** are needed to gradually increase overall investments by 2020 and beyond, in line with the EU's economic weight and investments on other continents.
Public and private **research and development investments in AI** in the EU last year were estimated to total EUR 4-5 billion.[206] **The EU as a whole (public and private sectors combined)** should aim to increase this investment to **at least EUR 20 billion by the end of 2020**. It should then **aim for more than EUR 20 billion per year over the following decade** (this objective does not pre-empt any decision to be taken with respect to the next EU multiannual financial framework).
The Commission will work with Member States on a coordinated plan to help align and step up investments, building on the declaration of cooperation signed on 10 April 2018.

Without such efforts, the EU risks losing out on the opportunities offered by AI, facing a brain-drain and being a consumer of solutions developed elsewhere. The EU should therefore strengthen its status as a research powerhouse while bringing more innovation to the market. A vast majority of European companies – whether large or small – should also adopt AI technologies.

Stepping up investments

2018-2020

To support joint efforts, **the Commission is increasing investments in AI** under the research and innovation framework programme Horizon 2020 to around **EUR 1.5 billion by the end of 2020** (this works out as an average of EUR 500 million per year and represents an increase of around 70%). Under the existing public-private partnerships (for example in robotics and big data), this investment will trigger an additional **EUR 2.5 billion** over the same period.

These investments will aim at consolidating research and innovation in AI, encouraging testing and experimentation, strengthening AI excellence research centres and starting efforts to bring AI to all potential users, with a focus on small and medium-sized enterprises.

If Member States[207] **and the private sector** (beyond established partnerships) **make similar investment efforts, the total investments in the EU** will grow to around EUR 7 billion per year, totalling **more than EUR 20 billion by the end of 2020**. This will position the EU well to further increase efforts over the next decade.

Strengthening research and innovation from the lab to the market

The Commission will support **AI technologies both in basic and industrial research**[208]. This includes investments in projects in key application areas such as health, connected and automated

[206] Estimate based on data on public and business spending in research and development (R&D) in information and communication technologies (ICT) (source: Prospective Insights in ICT R&D, PREDICT, European Commission) and the share of funding in AI as part of the Commission's research and development budget in information and communication technologies since 2014 (around 13%). Building on previous trends, a similar share is calculated for government budget allocations for research and development and business expenditure on research and development which represents the major part of investments (ca. EUR 4 billion, which is consistent with recent findings by McKinsey).

[207] For example, France has just announced a EUR 1.5 billion investment in AI over five years.

[208] The guiding principle of all support for AI-related research will be the development of "responsible AI", putting the human at the centre, see the Commission's "Responsible Research and Innovation" workstream: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

driving, agriculture, manufacturing, energy, next generation internet technologies, security and public administrations (including justice). Funding will also reinforce European strengths in embodied AI/robotics.

The Commission will also **support breakthrough market-creating innovation such as AI** through the pilot of the **European Innovation Council**.[209] A budget of EUR 2.7 billion is made available for 2018-2020 to support 1,000 potential breakthrough projects and 3,000 feasibility awards. This pilot scheme can be particularly helpful for AI development as AI technology is expected to be part of many projects, for applications in e.g. health, agriculture and manufacturing.

Funding in fundamental research is expected to be provided by the **European Research Council**, based on scientific excellence. **Marie Skłodowska-Curie actions** provide grants for all stages of researchers' careers and have supported research in AI in the past years.

Supporting AI research excellence centres across Europe

Building on Member States' efforts to **jointly establish AI-focused research centres**, the Commission will support and strengthen AI excellence centres across Europe. The Commission will also encourage and facilitate their collaboration and networking.

Bringing AI to all small businesses and potential users

Europe can only reap the full benefits of AI if it is available and accessible to all. The Commission will **facilitate access of all potential users, especially small and medium-sized enterprises, companies from non-tech sectors and public administrations, to the latest technologies and encourage them to test AI**. To this end, the Commission will support the development of an "AI-on-demand platform". This will provide a single access point for all users to relevant AI resources in the EU, including knowledge, data repositories, computing power (cloud, high performance computing), tools and algorithms. It will offer services and provide support to potential users of the technology, analyse the business case behind AI in their specific circumstances and help them to integrate AI solutions in their processes, products and services.

To facilitate access to the platform, the existing network of more than 400 Digital Innovation Hubs[210] will be instrumental. Further Hubs are coming on stream and a dedicated network of **Digital Innovation Hubs focused on AI** will be created.

Digital Innovation Hubs *help companies (especially small and medium-sized enterprises) to take advantage of digital opportunities. They offer expertise on technologies, testing, skills, business models, finance, market intelligence and networking.*

For example, a small company that produces metal parts for the automotive industry could consult the regional hub (which can be a science park for example) and ask for advice on how to improve the manufacturing process with AI. Experts from the hub would then visit the factory, analyse the production process, consult with other AI experts in the network of hubs, make a proposal and then implement it. These activities would be partially financed with EU money.

The Commission will also analyse systemic shifts in value chains in order to anticipate AI opportunities for small and medium-sized enterprises, pilot critical industrial AI applications in non-tech sectors, and reinforce the European advanced manufacturing support centre for small and medium-sized enterprises.

Supporting testing and experimentation

Testing of and experimenting with AI products and services is crucial to make them market-ready, ensure compliance with safety standards and rules as well as security by design and enable policymakers to gain experience with new technologies to devise suitable legal frameworks. The

[209] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/european-innovation-council-eic-pilot

[210] See also the Commission's Communication of 19 April 2016 on Digitising European Industry (COM/2016/0180 final) and list of hubs.

Commission will support the set-up of testing and experimentation infrastructures that are open to businesses of all sizes and from all regions. Building on the established network of Digital Innovation Hubs, a **first series of testing and experimentation infrastructures for AI** products and services will be set up in the areas of healthcare, transport, infrastructure inspection and maintenance, agrifood and agile production.

Attracting private investments

On top of investments under the research and innovation framework programme, a sufficient level of private investments in the AI transformation is crucial. The **European Fund for Strategic Investments** will be further mobilised to attract private investment to support the development and the uptake of AI, as part of the wider efforts to promote digitisation. The Commission will work with the European Investment Bank Group with the aim of reaching **at least EUR 500 million in total investments** in that area in the period 2018-2020. In addition, the European Commission and the European Investment Fund have just launched a EUR 2.1 billion Pan-European Venture Capital Funds-of-Funds programme – **VentureEU** – to boost investment in innovative startup and scale-up companies across Europe. The Commission also provides support as part of its **initiatives to digitise industry**[211].

In 2018-20[212], the Commission will invest around **EUR 1.5 billion** in:

- **research and innovation in AI technologies** to strengthen European industrial leadership, excellence in science, and support AI applications which address societal challenges in sectors such as health, transport and agrifood. The Commission will also support breakthrough, market-creating innovation through the pilot phase of the European Innovation Council;
- strengthening **AI research excellence centres**; and
- the **uptake of AI across Europe**, via a **toolbox for potential users, with a focus on small and medium-sized enterprises, non-tech companies and public administrations**: this will include an **AI-on-demand platform** giving support and easy access to the latest algorithms and expertise; a **network of AI-focused Digital Innovation Hubs** facilitating **testing and experimentation**; and the set-up of **industrial data platforms** offering high quality datasets.

In addition, the Commission aims to stimulate more private investments in AI under the **European Fund for Strategic Investments** (**at least EUR 500 million** in 2018-20).

Beyond 2020

Commission proposals under the **next EU multiannual financial framework (2021-2027)** will open the door to investments into:

- **upgrading** the pan-European **network of AI excellence centres**;
- **research and innovation in fields such as explainable AI**[213]**, unsupervised machine learning, energy and data efficiency**[214]**;**

[211] The Commission has just launched the Strategic Forum for Important Projects of Common European Interest to identify and ensure appropriate large-scale finance for value chains of strategic importance for Europe including the integration of AI to strengthen EU industrial leadership. Moreover, the Commission supports and facilitates inter-regional partnerships for investments in advanced technologies and AI through its Smart Specialisation Platform on Industrial Modernisation.

[212] Actions will stem from the work programme Horizon 2020. They will be financed within the current financial programming envelope and subject to future revision of the work programme in the frame of the comitology procedure.

[213] In order to increase transparency and minimise the risk of bias or error, AI systems should be developed in a manner which allows humans to understand (the basis of) their actions.

[214] These being methods to use less data in order to train AIs.

- additional Digital Innovation Hubs, world-leading **testing and experimentation facilities** in areas such as transport, healthcare, agrifood and manufacturing, supported by **regulatory sandboxes**[215];
- supporting the adoption of AI by organisations across all sectors, including **public interest applications**, through co-investment with Member States;
- exploring joint **innovation procurement** for the use and development of AI; and
- a **support centre for data sharing**, which will be closely linked with **the AI-on-demand** platform to facilitate development of business and public sector applications.

The Commission also intends to continue its support for technologies and infrastructure that underpin and enable AI such as high-performance computing, microelectronics, photonics, quantum technologies, the Internet of Things and cloud.

In doing so, the Commission will support more **energy-efficient technologies** and infrastructure, **making the AI value chain greener**.

Making more data available

AI needs vast amounts of data to be developed. Machine learning, a type of AI, works by identifying patterns in available data and then applying the knowledge to new data.[216] The larger a data set, the better even subtle relations in the data can be discovered. When it comes to using AI, data-rich environments also provide for more opportunities. This is because data is the way the algorithm learns about and interacts with its environment. For example, if all machines and processes in a factory continuously produce data, it is likely that further automation and optimisation can be achieved with the help of AI. In an analog setting, e.g. in a paper-based operation without digitised data about what is happening, that is not the case. In view of this, access to data is a key ingredient for a competitive AI landscape, which the EU should facilitate.

> ***Deep learning*** *has been a game-changer for AI with a tremendous improvement in performance for specific tasks such as image or speech recognition, or machine translation.*
>
> *Training a deep learning algorithm to classify objects works by exposing it to a large number of labelled examples (e.g. pictures) that are correctly categorised (e.g. pictures of planes).*
>
> *Once trained, algorithms can correctly classify objects that they have never seen, in some cases with accuracies that exceed those of humans.*
>
> *Significant advances in these technologies have been made through the use of large data sets and unprecedented computing power.*

The EU has made significant efforts over the past 15 years **to open up public sector information and publicly funded research results** for re-use, such as data generated by the EU's space programmes (Copernicus[217], Galileo). With its initiative to improve the accessibility and re-usability of such data, this body of data will grow further.

Public policy should also encourage **the wider availability of privately-held data**, while ensuring full respect for legislation on the protection of personal data. The Commission calls on

[215] These are testing grounds for new business models that are not (yet) regulated.

[216] Sometimes finding the pattern is itself the goal of the activity: in text and data mining, researchers use algorithms to "read" a large numbers of texts (e.g. scientific papers on chemistry) and automatically extract knowledge (e.g. finding facts that are not explicitly stated in any one of the papers but can be derived from the whole corpus). The Commission introduced an exception for text and data mining as part of the modernisation of EU copyright rules.

[217] Copernicus Data and Information Access Services: http://copernicus.eu/news/upcoming-copernicus-data-and-information-access-services-dias

companies to recognise the importance of non-personal data re-use, including for AI training purposes.

A new **support centre for data sharing** will provide public authorities and companies with legal and technical support when trying to access data from public sector bodies and companies.

The Commission will continue to study how more data can be made available.

Alongside this Communication, the Commission has put forward a set of initiatives to grow the European data space[218]. These are:

- an **updated Directive on public sector information**, e.g. traffic, meteorological, economic and financial data or business registers;
- **guidance on sharing private sector data in the economy** (including industrial data);
- an **updated Recommendation on access to and preservation of scientific information**; and
- a **Communication on the digital transformation of health and care**, including sharing of genomic and other health data sets.

3.2. Preparing for socioeconomic changes

Throughout history, the emergence of new technologies – from electricity to the internet – has changed the nature of work. It has brought major benefits to our society and economy, but also raised concerns. The emergence of automation, robotics and AI is transforming the labour market, and it is essential for the EU to manage this shift.

These technologies can make the life of workers easier. They can, for example, help them with repetitive, strenuous and even dangerous tasks (for example cleaning unsafe or difficult to access locations such as industrial pipes). They can also help summarise large amounts of data, provide more accurate information and suggest decisions, including using AI to assist doctors with diagnosis. They ultimately help to **enhance people's abilities**. Against the background of an ageing society, AI can provide new solutions to support more people to participate and remain in the labour market, including persons with disabilities. **New jobs and tasks will emerge as a result of AI**, some of which are difficult, or even impossible to predict. Other jobs and tasks will be replaced. While the exact quantification of AI's impact on jobs is difficult to determine at this stage, the need for action is clear.

Overall there are three main challenges for the EU – highlighting the fundamental role of education and training, including of teachers and trainers themselves, for which responsibility lies with Member States. The first challenge is to **prepare the society as a whole**. This means helping all Europeans to develop basic digital skills, as well as skills which are complementary to and cannot be replaced by any machine such as critical thinking, creativity or management. Secondly, the EU needs to focus efforts to help workers in **jobs which are likely to be the most transformed or to disappear** due to automation, robotics and AI. This is also about ensuring access for all citizens, including workers and the self-employed[219], to social protection[220], in line with the **European Pillar of Social Rights**. Finally, the EU needs to **train more specialists in AI**, building on its long tradition of academic excellence, create the right environment for them to work in the EU and attract more talent from abroad.

[218] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy
[219] http://ec.europa.eu/social/BlobServlet?docId=19158&langId=en
[220] Automation may impact the way social protection is financed, necessitating a proper reflection on the sustainability and adequacy of social security systems.

Leaving no one behind

In 2016, the European Commission launched a comprehensive plan to help equip people with the right skills for the evolving labour market: a **New Skills Agenda for Europe**[221]. As part of this agenda, the Commission issued a Recommendation for Member States on "Upskilling Pathways: New Opportunities for Adults" to improve their basic literacy, numeracy and digital skills. A Recommendation was also adopted on key competences for lifelong learning, focusing notably on the acquisition of competences in sciences, technology, engineering and mathematics (STEM), digital competences, entrepreneurship and creativity. The Commission also presented a Digital Education Action Plan[222] which aims to foster digital skills and competences for all citizens. This plan explores the impact of AI in education and training through pilots.

While digitisation is affecting the structure of the labour market in particular through the automation of middle-skilled jobs, AI could have a more significant impact on lower skilled jobs.[223] If not addressed early and proactively, this may exacerbate inequalities between people, regions and industries in the EU.

To manage the AI transformation, workers whose jobs are changing or may disappear due to automation must have every opportunity to acquire the skills and knowledge they need, to master new technology and be supported during labour market transitions. This anticipatory approach and focus on investing in people is a cornerstone of a human-centric, inclusive approach to AI, and will require a significant investment. National schemes will be essential for providing such up-skilling and training. They will benefit from support by the European Structural and Investment Funds (supporting skills development with EUR 27 billion over the period 2014-2020, out of which the European Social Fund invests 2.3 billion specifically in digital skills) and should also benefit from support from the private sector. The Commission will also continue to support research into human-AI interaction and cooperation.

Nurturing talent, diversity and interdisciplinarity

AI has brought about new job profiles, including in the area of developing machine-learning algorithms and other digital innovations.[224] Overall, the number of specialists in information and communication technologies in the EU has grown annually by 5% since 2011, creating 1.8 million jobs and rapidly increasing its share of total employment from 3% to 3.7% in just five years. There are at least 350,000 vacancies for such professionals in Europe, pointing to significant skills gaps.[225] This is why Europe should strive to **increase the number of people trained in AI** and **encourage diversity**. More women and people of diverse backgrounds, including people with disabilities, need to be involved in the development of AI, starting from inclusive AI education and training, in order to ensure that AI is non-discriminatory and inclusive. **Interdisciplinarity** should also be supported (by encouraging joint degrees, for example in law or psychology and AI). The importance of ethics in the development and use of new technologies should also be featured in programmes and courses. And it is not only about training the best talent, but also creating an **attractive environment for them to stay in the EU**.

Initiatives to encourage more young people to choose AI subjects and related fields as a career should be promoted. The Commission has recently launched the "Digital Opportunity Traineeships"[226], supporting internships aimed at acquiring advanced digital skills, and a number of actions of the Digital Skills and Jobs Coalition[227] aim at spreading coding skills and increasing the number of experts in digital.

---

[221] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0381

[222] https://ec.europa.eu/education/sites/education/files/digital-education-action-plan.pdf

[223] Organisation for Economic Co-operation and Development, "Automation, skills use and training", 2018.

[224] https://www.cognizant.com/whitepapers/21-jobs-of-the-future-a-guide-to-getting-and-staying-employed-over-the-next-10-years-codex3049.pdf

[225] http://www.pocbigdata.eu/monitorICTonlinevacancies/general_info/

[226] https://ec.europa.eu/digital-single-market/en/digital-opportunity-traineeships-boosting-digital-skills-job

[227] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition

Ensuring that workers are given the chance to adapt and to have access to new opportunities will be crucial for people to accept AI. Like any other technology, AI is not just imposed on society. It is up to governments, in dialogue with the social partners and civil society bodies, to collectively steer the process to ensure that its benefits are widely shared, that all citizens are suitably equipped to take full advantage of this technology and that a broader reflection on potentially deeper societal changes is taking place.

In 2018, in order to support the efforts of Member States which are responsible for labour and education policies, the Commission will:

- set up **dedicated (re-)training schemes** in connection with the Blueprint on sectoral cooperation on skills[228] – which brings together businesses, trade unions, higher education institutions and public authorities – for professional profiles which are at risk of being automated, with financial support from the European Social Fund[229];
- gather detailed analysis and expert inputs to **anticipate the changes on the labour market and the skills mismatch** across the EU, and inform decision-making at EU, national and local levels. More specifically, the Commission will (i) publish a foresight report on the impact of AI in education; (ii) launch pilots to predict the training requirements for future competence profiles; and (iii) publish an expert **report addressing the labour market impacts of AI**, with **recommendations**;
- support Digital Opportunity **Traineeships** (2018-20) **in advanced digital skills** for students and fresh graduates;
- encourage, through the Digital Skills and Jobs Coalition, **business-education partnerships** to take steps to attract and retain more AI talent and to foster continued collaboration; and
- invite **social partners** to include AI and its impact on the economy and employment, including the importance of diversity and gender balance in AI jobs, in their joint work programmes at sectoral and cross-sectoral level where relevant.

The **European Institute of Innovation and Technology** will integrate **AI across curricula in the education courses it supports**, in order to contribute to developing a talent pool for AI in Europe.

Proposals under the next EU multiannual financial framework (2021-2027) will include strengthened support for the acquisition of advanced digital skills including AI-specific expertise.

The Commission also intends to broaden the scope of the current European Globalisation Adjustment Fund beyond redundancies caused by delocalisation, including to those resulting from digitisation and automation.

3.3. Ensuring an appropriate ethical and legal framework

An environment of trust and accountability around the development and use of AI is needed.

The **values** set out in Article 2 of the Treaty on European Union constitute the foundation of the rights enjoyed by those living in the Union. In addition, the **EU Charter of Fundamental Rights** brings together all the personal, civic, political, economic and social rights enjoyed by people within the EU in a single text.

The EU has a strong and balanced regulatory framework to build on, which can set the global standard for a sustainable approach to this technology. The Union has **high standards in terms**

[228] http://ec.europa.eu/social/main.jsp?catId=1415&langId=en
[229] The cooperation now focuses on the automotive, maritime technology, space, textile and tourism sectors, and will address six other sectors in the future: additive manufacturing; construction; green technologies and renewable energy; maritime shipping; paper-based value chain; steel industry.

of safety and product liability. The first EU-wide rules on **network and information systems security** and stronger rules on the **protection of personal data** will become a reality in May 2018.

The **General Data Protection Regulation** ensures a high standard of personal data protection, including the principles of data protection by design and by default. It guarantees the free flow of personal data within the Union. It contains provisions on decision-making based solely on automated processing, including profiling. In such cases, data subjects have the **right to be provided with meaningful information** about the logic involved in the decision.[230] The General Data Protection Regulation also gives individuals the right not to be subject solely to automated decision-making, except in certain situations.[231] The Commission will closely follow the Regulation's application in the context of AI and calls on the national data protection authorities and the European Data Protection Board to do the same.

The Commission has also put forward a series of proposals under the **Digital Single Market** strategy that will be a key enabler for the development of AI, such as the Regulation on the free flow of non-personal data, and that will strengthen trust in the online world, such as the ePrivacy Regulation and the Cybersecurity Act. These proposals need to be adopted as soon as possible. This is essential as **citizens and businesses alike need to be able to trust the technology they interact with**, have a predictable legal environment and rely on effective safeguards protecting fundamental rights and freedoms.

To further strengthen trust, people also need to understand how the technology works, hence the importance of research into the **explainability of AI systems**. Indeed, in order to increase transparency and minimise the risk of bias or error, AI systems should be developed in a manner which allows humans to understand (the basis of) their actions.

Like every technology or tool, AI can be used to positive but also to malicious ends. Whilst AI clearly generates new opportunities, it also poses challenges and risks, for example in the areas of safety and liability, security (criminal use or attacks), bias[232] and discrimination.

Reflection will be needed on interactions between AI and intellectual property rights, from the perspective of both intellectual property offices and users, with a view to fostering innovation and legal certainty in a balanced way.[233]

Draft AI ethics guidelines

As a first step to address ethical concerns, **draft AI ethics guidelines will be developed by the end of the year**, with due regard to the Charter of Fundamental Rights of the European Union. The Commission will bring together all relevant stakeholders in order to help develop these draft guidelines.

The draft guidelines will address issues such as the future of work, fairness, safety, security, social inclusion and algorithmic transparency. More broadly, they will look at the impact on fundamental rights, including privacy, dignity, consumer protection and non-discrimination. They will build on the work of the European Group on Ethics in Science and New Technologies[234] and take inspiration from other similar efforts.[235] Companies, academic institutions, and other

[230] Articles 13 (2) f), 14 (2) g) and 15 (1) h) of the General Data Protection Regulation.
[231] Article 22 of the General Data Protection Regulation.
[232] Depending on the data input that is used to train AI systems, their outputs can be biased.
[233] Using AI to create works can have implications on intellectual property, with questions arising for instance on patentability, copyright and right ownership.
[234] The European Group on Ethics in Science and New Technologies is an advisory group of the Commission.
[235] At the EU level, the EU Fundamental Rights Agency will carry out an assessment of the current challenges faced by producers and users of new technology with respect of fundamental rights compliance. The European Group on Ethics in Science and New Technologies also published a relevant statement on AI, Robotics and 'Autonomous' Systems on 9 March 2018. Examples of international efforts: Asilomar AI principles (https://futureoflife.org/ai-principles/), Montréal Declaration for Responsible AI draft

organisations from civil society bodies will be invited to contribute. In parallel, the Commission will continue its work towards progress on ethics at international level[236].

While self-regulation can provide a first set of benchmarks against which emerging applications and outcomes can be assessed, public authorities must ensure that the regulatory frameworks for developing and using of AI technologies are in line with these values and fundamental rights. The Commission will monitor developments and, if necessary, review existing legal frameworks to better adapt them to specific challenges, in particular to ensure the respect of the Union's basic values and fundamental rights.

Safety and liability

The emergence of AI, in particular the complex enabling ecosystem and the feature of autonomous decision-making, requires a reflection about the suitability of some established rules on safety and civil law questions on liability.

For instance, advanced robots and Internet of Things products empowered by AI may act in ways that were not envisaged at the time when the system was first put into operation. Given AI's widespread uses, both horizontal and sectoral rules may need to be reviewed[237].

The EU safety framework[238] already addresses the intended use and foreseeable (mis)use of products when placed on the market. This has led to the development of a solid body of standards in the area of AI-enabled devices that is continuously being adapted in line with technological progress..

The further development and promotion of such safety standards and support in EU and international standardisation organisations will help enable European businesses to benefit from a competitive advantage, and increase consumer trust[239].

The Commission is currently assessing whether the safety and national and EU liability frameworks are fit for purpose in light of these new challenges or whether any gaps should be addressed. A high level of safety and an efficient redress mechanism for victims in case of damages helps to build user trust and social acceptance of these technologies.

Evaluations of the Product Liability Directive[240] and the Machinery Directive have already been conducted.[241] An initial assessment was also carried out on the current liability frameworks in

principles (https://www.montrealdeclaration-responsibleai.com/), UNI Global Union Top 10 Principles for Ethical AI (http://www.thefutureworldofwork.org/opinions/10-principles-for-ethical-ai/).

[236] The European Commission's International Dialogue on Bioethics and Ethics in Science and New Technologies brings together the National Ethics Councils of EU Member States and of third countries, to work together on those matters of common concern.

[237] For any new regulatory proposals that shall be needed to address emerging issues resulting from AI and related technologies, the Commission applies the Innovation Principle, a set of tools and guidelines that was developed to ensure that all Commission initiatives are innovation friendly: https://ec.europa.eu/epsc/publications/strategic-notes/towards-innovation-principle-endorsed-better-regulation_en

[238] For example, the Machinery Directive, the Radio Equipment Directive, the General Product Safety Directive as well as specific safety rules for example for medical devices or toys.

[239] Standards should also cover interoperability, which is crucial for offering consumers greater choices and ensuring fair competition.

[240] The Product Liability Directive states that if a defective product causes any damage to consumers or their property, the producer has to provide compensation irrespectively of whether there is negligence or fault on their part.

[241] The evaluation of the Machinery Directive indicates that some provisions do not explicitly address certain aspects of emerging digital technologies, and the Commission will examine whether this requires legislative changes. On the evaluation of the Product Liability Directive, the Commission will issue an interpretative guidance document, clarifying important concepts in the Directive.

light of AI and emerging technologies.[242] An expert group will help the Commission to analyse these challenges further.[243]

Empowering individuals and consumers to make the most of AI

The large-scale use of AI-enabled tools in business-to-consumer transactions needs to be fair, transparent and compliant with consumer legislation. Consumers should receive clear information on the use, features and properties of AI-enabled products. Individuals should be able to control the data generated by using these tools and should know whether they are communicating with a machine or another human. In particular, when interacting with an automated system, consideration should be given to when users should be informed on how to reach a human and how to ensure that a system's decisions can be checked or corrected.

The Commission will:

- set a framework for stakeholders and experts – the European AI Alliance – to develop **draft AI ethics guidelines**, with due regard to fundamental rights, **by the end of the year**, in cooperation with the European Group on Ethics in Science and New Technologies;
- **issue a guidance document on the interpretation of the Product Liability Directive** in light of technological developments **by mid-2019**. This will seek to ensure legal clarity for consumers and producers in case of defective products;
- publish, **by mid-2019**, a **report on** the broader **implications** for, potential **gaps in and orientations for,** the **liability** and **safety frameworks** for AI, Internet of Things and robotics;
- support research in the development of **explainable AI** and implement a pilot project proposed by the European Parliament on **Algorithmic Awareness Building**[244], to gather a solid evidence-base and support the design of policy responses to the challenges brought by automated decision-making, including biases and discrimination (2018-2019); and
- support national and EU-level **consumer organisations and data protection supervising authorities** in building an understanding of AI-powered applications with the input of the European Consumer Consultative Group and of the European Data Protection Board.

3.4. Joining forces

Engaging Member States

Several Member States have developed or are working towards strategies to support AI. On 29 March 2018, France presented its national strategy for AI, building on the Villani report.[245] Germany, following the example of "Industrie 4.0", has set up a platform on learning systems to enable a strategic dialogue between academia, industry and the government, and it has put forward a report on the ethics of automated and connected driving.[246] Finland has put forward its 'Tekoälyaika' strategy to make it a leader in the field.[247] Every Member State is encouraged to have an AI strategy, including on investment.

Sharing best practices, identifying synergies and aligning action where relevant will maximise the impact of investments in AI and help the EU as a whole to compete globally. Cooperating on interoperability and data sets, and working together on legal solutions will prevent a fragmentation of the single market and therefore fuel the emergence of AI startups. 24 Member States and Norway have already committed to joining forces on AI and entering into a strategic

[242] See the Staff Working Document on Liability accompanying this Communication (SWD (2018)137).
[243] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=615947
[244] https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building
[245] https://www.aiforhumanity.fr
[246] https://www.plattform-lernende-systeme.de
[247] https://tekoalyaika.fi/

dialogue with the Commission.[248] **The Commission will facilitate this dialogue and aim to agree a coordinated plan on AI with Member States by the end of the year.**

Engaging stakeholders: setting up a European AI Alliance

Given the scale of the challenge associated with AI, the full mobilisation of a diverse set of participants, including businesses, consumer organisations, trade unions, and other representatives of civil society bodies is essential. The Commission will therefore facilitate the creation and operation of **a broad multi-stakeholder platform,** the **European AI Alliance**, to work on all aspects of AI.[249] The Commission will also facilitate interactions of the Alliance with the European Parliament, Member States, the European Economic and Social Committee, the Committee of the Regions as well as international organisations. The Alliance will be a space for sharing best practices, encourage private investments and activities related to the development of AI.

Monitoring AI development and uptake

Many of today's debates about AI are based on opinions, hearsay and assumptions – not always on facts and science. To ensure quality input and to inform policy-making, the Commission will monitor the uptake of AI applications across the economy and identify potential shifts in industrial value chains caused by AI as well as societal and legal developments and the situation on the labour market. It will also benchmark the technical capabilities of AI components and systems to give a realistic understanding of where the technology stands, and help increase public awareness.[250] The Commission will also regularly assess progress towards the objectives and the initiatives set out in this Communication.

International outreach

International discussions on AI have intensified after Japan's G7 Presidency put the topic on the table in 2016. The EU has supported these discussions both in G7 ministerial meetings and at the Organisation for Economic Co-operation and Development, which is becoming a major international venue to discuss this topic. More specifically, the Commission has encouraged the discussions on AI ethics within the G7.

With AI being easily tradeable across borders, only global solutions will be sustainable in this domain. The G7/G20, United Nations and Organisation for Economic Co-operation and Development have begun to address the role of AI, including in the military domain. The EU will continue to encourage discussions on AI and its various dimensions – including research and innovation cooperation as well as competitiveness – in such fora. It will promote the use of AI, and technologies in general, to help solve global challenges, support the implementation of the Paris Climate agreement and achieve the United Nations Sustainable Development Goals.

The EU can make a unique contribution to the worldwide debate on AI based on its values and fundamental rights.

---

[248] https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

[249] https://ec.europa.eu/digital-single-market/en/news/call-high-level-expert-group-artificial-intelligence

[250] This work shall also be informed by the EU Agency on Fundamental Rights.

- **By the end of the year**, the Commission will work, as part of the existing European platform of national initiatives to digitise industry, on a **coordinated plan with Member States** in order to maximise the impact of investments at EU and national levels, exchange on the best way for governments to prepare Europeans for the AI transformation and address legal and ethical considerations. In parallel, the Commission will **systematically monitor AI-related developments**, e.g. policy initiatives in the Member States, AI uptake and its impact on labour markets as well as AI capabilities, including high-level benchmarking, showcasing current capabilities and developing an AI index in order to inform the discussions.
- **By July 2018**, the **European AI Alliance** will be set up. It will involve all relevant stakeholders to gather input, exchange views, develop and implement common measures to encourage the development and use of AI.

4. Conclusion

The EU has a strong scientific and industrial base to build on, with leading research labs and universities, recognised leadership in robotics as well as innovative startups. It has a comprehensive legal framework which protects consumers while promoting innovation and it is making progress in creating a Digital Single Market. **The main ingredients are there for the EU to become a leader in the AI revolution**, in its own way and based on its values.

The approach to AI described in this document shows the way forward and highlights the need to join forces at European level, to ensure that all Europeans are part of the digital transformation, that adequate resources are devoted to AI and that the Union's values and fundamental rights are at the forefront of the AI landscape.

Together, we can place the power of AI at the service of human progress.

Commission Staff Working Document on the liability for emerging digital technologies

Commission Staff Working Document on the liability for emerging digital technologies accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe {COM(2018) 237 final}

1. Introduction

Emerging digital technologies, such as the Internet of Things (IoT), Artificial Intelligence, advanced robotics and autonomous systems, lead to the creation of new products and services that allow for new opportunities for our economy and society. These new products and services can create new systems and complex environments that significantly improve our daily life.

An example is the smart home environment. This environment comprises connected and intelligent products (like smart fridges, smart meters, smart doors or smart fire alarms), which collect data through sensors, interact autonomously with each other and with external actors and use cloud services, embedded and non-embedded software for the provision of sophisticated hybrids between products and services.

In order to fully benefit from the opportunities presented by these new products and services, stimulating investment in emerging digital technologies is critical. A clear and stable legal framework will stimulate investment and, in combination with research and innovation, will help bring the benefits of these technologies to every business and citizen.

These new products and services are not inherently less safe than traditional products. Consumers' trust and the uptake of these technologies will depend on whether they are perceived to be safe and on whether the legal framework is considered clear and effective to provide remedies to victims. Clearly, the way in which technologies and tools are used is important for safety and liability aspects. When designing new technologies, it is important to consider also occupational health and safety aspects, in particular, in relation to ergonomics and mental stress. The liability framework that is currently existing in the European Union – as will be described further in this document - is a stable framework that incites investment, innovation and risk-taking.

Nevertheless, a reflection on future needs and developments is needed, not only from the perspective of the victim i.e. in order to ensure equitable remedies, compensation and allocation of responsibility, but also from the perspective of the innovators and companies operating in the EU as legal certainty is a key element for good business development.

In certain cases, when digital technology products or services cause a damage, the allocation of liability[251] may be complex due to their specific characteristics. In addition, ensuring their safety over their lifetime is important, as it can prevent or reduce potential damages and liability issues. It is therefore necessary to examine whether existing rules at EU and national level for safety and for the allocation of liability and the conditions, under which a victim is entitled to obtain compensation for damages caused by products and services stemming from emerging digital technologies, are appropriate and whether, for the producers and services providers, the framework continues to deliver an adequate level of legal certainty.

[251] For the purpose of this document, 'liability' means the responsibility of one party for harm or damage caused to another party, which may be a cause for compensation, financially or otherwise, by the former to the latter.

The Commission has engaged in a series of activities since 2015 which included to look into the issue of liability, also in relation to cybersecurity[252], in various Communications and strategic documents, to ensure legal certainty for the rollout and uptake of emerging digital technologies and to fully exploit their potential, as explained in the Communication "Artificial intelligence for Europe"[253].

In particular, the Digital Single Market Strategy (DSM)[254] emphasised the importance of legal certainty for the rollout of the Internet of Things (IoT)[255] and the Communication on "Building a European Data Economy"[256] committed to assess whether the current EU legal rules for product liability are fit for purpose, when damages occur in the context of the use of IoT and autonomous systems. In May 2017, the DSM mid-term review[257] announced that the Commission will consider the possible need to adapt the current legal framework to take account of emerging digital technologies, especially from the angle of civil law liability and taking into account the results of the ongoing evaluation of the Product Liability Directive[258] and the Machinery Directive[259].

The European Parliament issued a Resolution[260] calling for updated civil liability rules that duly take into account the development of autonomous and cognitive features in cars and robots including their safety aspects.

The objective of this document is therefore to provide a first mapping of liability challenges that occur in the context of emerging digital technologies. It builds on preliminary work, such as studies[261], public consultations and internal legal analysis, and provides a basis for the work of an Expert Group on "Liability and New Technologies" which will provide the Commission with expertise on the applicability of the Product Liability Directive to traditional products, new technologies and new societal challenges. The work of this group will also aim at providing the Commission with input relating to the different objectives, as set out in the policy documents referred to above and to consider possible adaptations of the current framework, in order to achieve clarity that would help stimulate investment in emerging digital technologies and to ensure that adequate redress mechanisms are in place in case of damages caused by products and services stemming from them.

---

[252] Joint Communication to the European Parliament and the Council on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final.
[253] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Artificial intelligence for Europe, COM(2018) 237 final.
[254] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A Digital Single Market Strategy for Europe, COM(2015) 192 final.
[255] Commission Staff Working Document on Advancing the Internet of Things in Europe, accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Digitising European Industry - Reaping the full benefits of a Digital Single Market, SWD(2016) 110 final.
[256] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Building a European Data Economy", COM(2017) 9 final.
[257] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All, COM(2017) 228 final.
[258] EU legislation on liability for defective products. Available at: http://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en.
[259] EU Machinery Legislation. Available at: http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en.
[260] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL).
[261] The publication of the final reports of two relevant studies is envisaged for June 2018.

As product liability and product safety are closely linked, Chapter 2 of the document outlines boththe existing safety and liability frameworks, which are pillars of the internal market. The EU approach to the internal market is based on common safety rules, underpinned by provisions on product liability, while the regime for contractual or extra-contractual liability for services and the regime for specific contractual or extra-contractual liability for products are left to national law. Chapter 3 presents the specific characteristics of emerging digital technologies: increasing level of complexity and variety of ecosystems, actors and value chains; autonomy in decision making and actuating; generation, processing and reliance of big volumes of data; and openness to software extensions, updates and patches after the products have been put into circulation[262]. The document then develops a number of brief theoretical case studies that aim at exemplifying the above specific characteristics, and at discussing the extent to which they could be covered by the existing rules and the impact they may have on the parties involved. Chapter 4 and 5 puts forward a series of questions for further reflection and analysis in relation to the existing elements and concepts and to wider issues, including cybersecurity as well as outlines next steps. The views expressed in this document should be understood as the Commission's services analysis of the matters under discussion, and do not constitute political commitments from the part of the Commission.

2. Landscape of Existing applicable rules and underlying principles from existing legislation or jurisprudence

Product safety and liability are complementary legal frameworks aiming to provide trust and safety to consumers. EU product safety legislation aims at ensuring that only safe products can be placed on the internal market of the Union. EU product liability legislation[263] provides for liability of producers of defective products that cause damage to natural persons or their property. In addition, various national liability regimes may apply if damage occurs.

2.1 Overview of relevant elements of safety rules applicable in the context of emerging digital technologies at EU level

Emerging digital technologies, such as IoT, AI-powered advanced robots and autonomous self-learning systems, must meet the essential health and safety requirements laid down in the applicable EU safety legislation[264] which ensures a single market for a wide range of equipment and machines, such as for instance Directive (EC) 2006/42[265] on machinery (which is the relevant safety legislation for robots), Directive 2014/53/EU on radio equipment[266], hereinafter referred to as the "Radio Equipment Directive" (which applies to all products, including embedded software, using the radio frequency spectrum), Council Directive 90/385/EEC on Active Implantable Medical Devices (AIMDD)[267], the Council Directive 93/42/EEC on Medical Devices (MDD)[268], Council Directive 98/79/EC on In Vitro Diagnostic Medical Devices (IVDMD)[269], as well

[262] A more detailed description of these specific characteristics per technology is given in Annex I.
[263] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29–33).
[264] A more comprehensive list of EU relevant legislation is included in Annex II.
[265] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) (OJ L 157, 9.6.2006, p. 24–86).
[266] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62–106).
[267] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (OJ L 189, 20.7.1990, p. 17–36).
[268] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p.1-43).
[269] Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices (OJ L 331, 7.12.1998, p. 1-37).

as the Council Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work.[270]

Alongside product harmonisation legislation, Directive 2001/95/EC of the European Parliament and the Council of 3 December 2001 on general product safety aims to ensure that only safe consumer products are placed on the market and acts as a safety net role for products and risks not covered by the harmonisation legislation.

Emerging digital technologies are also being incorporated in other products; therefore, other EU legislative instruments also apply. In the framework of the Union harmonisation legislation on products, manufacturers must ensure that products meet the essential health and safety requirements by following the applicable conformity assessment procedures, involving in some cases a conformity assessment body, and must keep the technical documentation about the products that they place on the market. These rules apply when the products are placed on the market and in some cases during the lifecycle of the product. They must be taken into consideration when a liability problem arises in relation to safety issues during the lifecycle of the product.

Currently, the production of European harmonised standards for IoT, AI-powered advanced robots and autonomous systems is ongoing. European Standardization Organisations draw up these standards in order to offer a level playing field and a competitive advantage to European manufacturers. These standards would offer presumption of conformity with the European safety legislation, under which they are developed, in particular under the Machinery Directive 2006/42/EC and the Radio Equipment Directive 2014/53/EU. The European Standardization Organizations are also working on standards for "combined" products, i.e. where several pieces of EU safety legislation apply.

Potential connectivity issues may arise in products currently on the market. The Commission has already been empowered under the Radio Equipment Directive 2014/53/EU (Article 3(3)) to ensure, for instance, that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software with the applicable safety requirements has been demonstrated (Article 3(3)(i)). The Expert Group on Reconfigurable Radio Systems is currently working to help the Commission to assess the possibility of adopting one or more delegated acts in that respect. Several stakeholders have already requested to start a similar exercise on other delegated provisions of this Directive, with the aim to specify the categories or classes of radio equipment concerned by the requirement to support certain features ensuring protection from frauds, to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected, to interwork with other radio equipment or not to misuse network resources.

2.2 Underlying principles of the extra-contractual liability rules applicable in the context of emerging digital technologies at EU and MS level

Extra-contractual liability relates to the civil law responsibility for damage caused outside the context of a contract (the damage being caused by a violation of a right or legitimate interest protected by law). Extra-contractual liability can be imposed by general civil law rules or specific

[270] Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (OJ L 183, 29.06.1989, p. 1-8).

legislation. Product liability is a form of statutory extra-contractual liability referring to the civil liability of manufacturers.

EU level

At EU level, the product liability regime was introduced by the Product Liability Directive. It was conceived around the notion of movable products, most of which are tangible. It puts forward a horizontal approach in relation to assigning liability in the case of defects and is technology neutral. It covers all types of products, ranging from raw materials to complex industrial products, now including emerging digital technology products. It covers Business-to-Consumer (B2C) relations and provides a comparatively simple point of reference for both consumers and producers.

The Product Liability Directive establishes a liability of producers when defective products cause damages to victims (including personal injuries or death or damage to property). This is a strict liability regime, in that the injured person does not have to prove a fault of the producer. The injured person carries the burden of proof of the defect in the product, the actual damage and the causal link between the defect and the damage.

The Product Liability Directive has an all-encompassing definition of producer, against whom the injured party can bring its claim: the manufacturer of the product, the producer of any raw material or the manufacturer of a component part or any person who, by putting its name, trademark or any distinguishing feature on the product presents himself as the producer. Furthermore, without prejudice to the liability of the producer, the importer is deemed to be a producer. Finally, where the producer cannot be identified, each supplier of the product shall be treated as its producer unless he informs the injured person of the identity of the producer.

The Court of Justice indicated that the Directive applies to products used while providing any service but that the liability of a service provider does not fall within the scope of the Directive.[271] However, the Directive does not prevent Member States from applying national rules under which a service provider using a defective product is liable for a damage caused by such use.

The Product Liability Directive creates an exhaustive harmonisation for the matters that it explicitly covers[272].

National level

At national level, the rules implementing the Product Liability Directive coexist[273] with other extra-contractual liability rules that could also be invoked by victims of damages. The Product Liability Directive does not preclude the application of other systems of contractual or non-contractual liability based on other grounds, such as fault or a warranty in respect to latent defects[274]. As regards national extra-contractual liability rules, broadly speaking they could be

[271] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
[272] For instance, CJEU. Judgment of 25 April 2002. Case C-52/00. Commission of the European Communities v French Republic.
[273] According to Article 13 of the Product Liability Directive, the "Directive shall not affect any rights which an injured person may have according to the rules of the law of contractual or non-contractual liability or a special liability system existing at the moment when this Directive is notified".
[274] CJEU- Judgement of 25 April 2002. Case C-183/00 María Victoria González Sánchez v Medicina Asturiana SA. and Judgement of 20 November 2014, Case C-310/13, Novo Nordisk Pharma G.

classified into two categories depending on whether the compensation of the victim requires a fault of the person considered liable by the law or not.[275]

Fault-based extra-contractual liability

As a general rule in most jurisdictions, extra-contractual liability regimes are fault-based. This means that the fault of the author of the wrongful behaviour leading to a damage (which could be an act or an omission whether intentional or by negligence) is a necessary element to be proven for the liability claim to be successful.

It is typically up to the victim submitting a claim to provide the evidence needed to support his liability claim. There are situations, however, where national law introduces variations to facilitate the burden of proof of the victim. Such variations may consist in a presumption of fault by the wrongdoer (or a reversal of the burden of proof), whereby the wrongdoer is liable unless he proves that he was not in fault. The variations may respond to the logic that the general rule on the burden of proof needs to be altered so as to increase the possibility of compensation for the victim or at least balance the situation of disadvantage in which the victim would be pursuant to the ordinary regime. These variations may also reflect the circumstance that there may be an imbalance of information between the victim and the wrongdoer. The abovementioned variations may be linked to a diverse set of factual situations generating different types of risks and damages, such as the responsibility of the owner/possessor of the building in case of damages causes by his/her building (unless he/she proves that he/she observed appropriate care for the purpose of avoiding the damage)[276], the responsibility of a person carrying a dangerous activity (unless he/she proves that all appropriate measures to avoid the damage have been taken)[277], the responsibility of the employer/the principal for the act executed on his behalf or interest by his employees/agents (unless he proves that he used appropriate care in the selection and the management of the agent/employee)[278] or the responsibility of parents/tutors/guardians/teachers for damages caused by a minor, pupil, student/apprentice or mentally impaired person (unless they can prove that they were not able to prevent the damages from happening). [279]

Special regimes of strict liability (extra-contractual)

National legal systems may also provide for special regimes of strict liability. In most jurisdictions, strict liability is often defined as a liability that does not depend on a fault and the claimant needs only to prove the damage and the causal link.

The reversal of the burden of proof in the context of a fault-based extra-contractual liability and the principle of strict liability typically respond to a common rationale. They both aim overall at facilitating the compensation of the victim of damages in situations where the legislator considers it too burdensome or unbalanced to apply the general fault-based liability rule. Some forms of strict liability may go even a step further by linking liability simply to the materialization of a risk and/or making the discharge of liability either impossible or possible only under the proof that the damaging event was caused by an exceptional/unforeseen circumstance that could not be avoided. There may be also other cases where the risk of damage is linked to the unpredictability

[275] The analysis of relevant elements and underlying principles of national law undertaken in this section is purely illustrative and is not meant to provide a comprehensive or representative portrait of national liability regimes. The analysis is based solely on a limited sample of national legal regimes.
[276] Cf. for example Section 836 German Civil Code, Section 1319 of the Austrian General Civil Code, Article 2053 of the Italian Civil Code or Section 6:560(1) of the Hungarian Civil Code.
[277] Cf. for example Article 2050 Italian Civil Code.
[278] Cf. for example Section 831 of the German Civil Code; Section 1315 of Austrian General Civil Code; Sections 6:540(1) and 6:542(1) of the Hungarian Civil Code.
[279] Cf. for example Articles 2048 and 2047 of the Italian Civil Code; Section 832 of the German Civil Code.

of behaviour of specific risk groups, like animals or certain persons: in these cases liability may be attributed to the persons that are considered responsible to supervise the animal or the person, because it is them who should normally be in the condition to adopt measures to prevent or reduce the risk of damages. Finally, when the risk of damages is linked to dangerous activities, some jurisdictions may attribute liability to the person that carries out the activity (e.g. the operator of a nuclear power plant or of an aircraft or the driver of a car) or is ultimately responsible for the dangerous activity to happen (e.g. the owner of a vehicle). The rationale typically is that this person has created a risk, which materialises in a damage and at the same time also derives an economic benefit from this activity.

Special regimes of strict liability may apply to a diverse set of factual situations generating different types of risks and damages, such as the liability of the owners of animals for the damages caused by the animals under their custody[280]; the strict liability of the person responsible for carrying out an unspecified[281] or specified dangerous activity (for example the operation of nuclear power plants,[282] aircrafts[283] or motor vehicles[284]) or other cases linked to a legal or factual relationship between two persons or a person and an object, such as when the damages are caused by someone executing a task in the interest of someone else (employee/employer)[285] or by an object that is under his/her custody.[286]

While none of the above selection of national law provisions are specifically applicable to damages that may potentially be caused by emerging digital technologies, these provisions certainly constitute helpful precedents or points of reference to which one can turn to further a reflection about how to best address, from a normative standpoint, certain distinguishing elements of risks and damages created by the emerging digital technologies.

Several Member States have begun to consider the implications of emerging digital technologies on their national liability regimes. For instance, the Justice Ministers of the German federal states adopted a resolution in June 2017 calling for legislative action, including at EU level as needed, in the area of extra-contractual liability for the operation of autonomous systems. In particular in the area of autonomous cars, some Member States have introduced or proposed sector specific legislation. For example, Germany has amended its Street Traffic Act in order to allow autonomous cars to operate on the streets provided that a human driver is present to take over control at all times. Sweden has introduced a law which allows the testing of autonomous vehicles. In the UK, the government has proposed legislation which would amend insurance legislation in connection with the possible roll-out of autonomous vehicles.[287]

International level

Other countries in the world are also analysing the liability implications of emerging digital technologies. In the US, numerous states are addressing the need for legislation of autonomous

[280] Cf. for example Article 2052 of the Italian Civil Code; Section 833 of the German Civil Code; Section 6:562 of the Hungarian Civil Code.
[281] Cf. for instance Section 6:535(1) of the Hungarian Civil Code.
[282] Cf. for instance Section 3 of the German Atomic Energy Act, in connection with Article 3 of the Paris Convention on Third Party Liability in the Field of Nuclear Energy.
[283] Cf. for instance Section 33 of the German Air Traffic Act and Section 148 of Austrian Air Traffic Act. Third-party liability insurance is required in those cases.
[284] Cf. for instance Article 2054 of the Italian Civil Code; Section 7 of the German Road Traffic Act; Section 5 of the Austrian Railway and Motor Vehicle Liability Act; Hungarian law considers motor vehicles as dangerous operations. (Cf. in this regard Section 6:535(1) Civil Code.
[285] Cf. for instance Art. 2049 of the Italian Civil Code.
[286] Cf. for instance Art. 2051 of the Italian Civil Code.
[287] House of Commons Library, Briefing Paper, Automated and Electric Vehicles Bill 2017-19, 28 November 2017. Available at: http://researchbriefings.files.parliament.uk/documents/CBP-8118/CBP-8118.pdf.

vehicles, although laws vary widely among themselves since they address licensing, use or regulation issues. Outstanding concerns include questions of responsibility and liability, as well as data protection and cybersecurity threats. In Japan, the Ministry of Economy, Trade and Industry is discussing legal issues regarding AI from the perspective of rights and responsibilities, including liability.

3. The specific characteristics of emerging digital technologies

Emerging digital technologies show certain levels of complexity due to the interdependency between the different components and layers: i) the tangible parts/devices (sensors, actuators, hardware), ii) the different software components and applications, to iii) the data itself, iv) the data services (i.e. collection, processing, curating, analysing), and v) the connectivity features.

As it has also been the case in the past, any interdependency gives rise to a number of questions, among which, who should be held liable in case the technology causes a damage or how to identify the root cause of the problem. Nonetheless, as far as they constitute 'movable' items, IoT devices and any other items containing intangible elements or presenting connectivity features qualify as 'products' and defects in these products are covered by the Product Liability Directive.

Issues relating to liability when products involve third party components are not new. The producer needs to ensure the safety of the final product, and in turn, producers and sellers are responsible for any liability arising from the products placed on the market or sold to customers regardless of whether they include third party components. However, based on the specific characteristics of these emerging digital technologies, it should be examined whether, when products and services are increasingly connected and complex both in the design and the system integration, effective redress mechanisms for victims and legal certainty for producers are still ensured.

Furthermore, these technologies will encompass more and more the feature of autonomy. Advanced robots or devices empowered by AI and IoT will have increased capabilities to interpret the environment (via sensing, actuating, cognitive vision, machine learning, etc.), to interact with humans, to cooperate with other artefacts, to learn new behaviours and execute actions autonomously without human intervention. The more autonomous systems are, the less they depend on other actors (i.e. the manufacturer, the owner, the user, etc.) and the greater is their impact on their environment and on third parties.

Combined with self-learning and autonomy, the behaviour of these technologies may be difficult to predict. This could raise questions regarding liability, in situations where the damage caused by a machine operating with a certain degree of autonomy cannot be linked to a defect or a human wrongdoing (e.g. of the driver; the car manufacturer, etc.), but also in the wider context of safeguards to be introduced to ensure the safety of such technologies (e.g. should machines be allowed to freely learn from their context or should they be prevented from learning inadequate/dangerous behaviours). As a consequence, the question of how to attribute liability where the expected outcome of the technology was not identified either before the market launch or after that launch needs to be examined.

Moreover, digital technology products and services generate (e.g. via sensors) and/or process data (e.g. through actuators, algorithms). The availability and the quality of data is essential for their good functioning. Faulty or corrupted data (e.g. due to connectivity problems or when hacked) may render the system malfunctioning.

Providing data through an IoT system could be considered a service, and thus fall as such, outside the product liability and safety regimes. Therefore, where damage is caused by the supply of erroneous data or by a failure to supply data, allocating liability may become unclear and claims potentially difficult to enforce.

Finally, digital technology products are open to software extensions, updates and patches after they have been put into circulation. Any change to the software of the system may affect the behaviour of the entire system or of individual components or may extend its functionality. Software can be patched, updated or revised, by the producer of the system or of individual system components or by third parties, in a way that can affect the safety of these technologies. Updates would usually close safety holes through patches, but new codes also add or remove features in ways that change the risk profile of these technologies.

Contractual liability of a software provider depends to a large extent on its contractual obligations (e.g. to supply applications which provide a certain level of safety and cybersecurity as well as updates for a certain period of time). A failure to comply with these obligations may trigger contractual liability claims. Such liability claims will aim at remedies in case of non conformity with the contract, e.g. bringing it into conformity, price reduction or termination of the contract, or at damages for breach of contract. The contractual liability of a software provider may be limited to the extent its customer contributed to the actual damage, e.g. because he did not install an available update. The liability of the software provider may also be limited according to the terms of the contract, to the extent such contractual limitation is permitted by the applicable law. The extent to which extra-contractual liability claims can be raised in parallel with possible contractual liability depends on national law.[288]

4. Case studies analysis

4.1 Introduction

The potential of AI and IoT powered systems is immense and not yet fully known or predictable at this stage. It is already clear, however, that AI applications and systems can generate autonomous decision-making and autonomous behaviour in the physical environment in which they operate including physical contact with humans and their property. This inevitably carries an inherent risk of causing damage to a third party's physical integrity or property. Damages may also be caused by AI systems that are not embedded in a hardware structure, for example economic damage caused by an autonomous trading algorithm at the stock exchange.

Although fully autonomous systems or IoT devices are not yet part of everyday life for most people, it is possible to anticipate likely realistic scenarios raising civil liability questions based on the current state of technological development and of known testing and pilot projects. The following case studies offer a first, preliminary description of such civil liability questions. As there is not yet a mass roll-out of these new technologies, the analysis that follows cannot yet rely on specific liability cases or court decisions and therefore works with some inevitable assumptions and theoretical considerations. In particular, while being based on existing legal concepts and possible relevant interpretations, the analysis does not specifically target and is not premised upon specific national legal systems. The primary goal of the use cases is to prepare the ground for further reflection. These case studies should not be seen as an exhaustive list, these and other cases will be explored further in the expert group work.

[288] This issue is demonstrated in the case decided by the Court of Appeal in Ghent (Belgium) in December 2016. De Redactie, Geldboetes voor UZ Gent en 3 bedrijven voor foute hersenbestraling, 7 September 2015. Available at: http://deredactie.be/cm/vrtnieuws/regio/oostvlaanderen/1.2434505.

4.2 AI powered devices and systems

Autonomous unmanned aircraft (autonomous drones)

Unmanned aircraft[289], or for brevity and for the purposes of this Staff Working Document drones, represent a rapidly developing sector of aviation with great potential to create new jobs and economic growth in the EU. The Commission predicts that by 2035, the European drone sector will directly employ more than 100,000 people and have an economic impact exceeding €10 billion per year, mainly in services. Drones can potentially be used for various civil purposes such as package delivery, surveillance and monitoring, data collection, inspection, search and rescue or even passenger transport. Drones rely on several technological components like for instance sensors, actuators and software that overall enable the drone's operation. While the level of automation may vary depending on the specific application, fully autonomous drones already exist for instance for the delivery of packages.

This use case discusses possible liability scenarios in the context of the use of autonomous drones, to be intended as drones executing a certain activity - such as the delivery of a package - in a completely autonomous manner, from take-off, to selection of the route, avoidance of obstacles, landing, etc.

A parcel delivery drone that is flying autonomously from the seller's warehouse to the customer's dwelling may cause damage in a variety of ways. It may abruptly fall to the ground or collide in-air with another flying vessel or drop the package resulting in property damage or personal injury.

Without prejudice to any possible national legislation addressing the specific liability for autonomous drones, it can be reasonable to argue that autonomous drones are "aircrafts" and could therefore potentially be covered by national laws and international conventions regarding the liability for aircraft. In this respect, typically aircraft are subject to a strict liability regime and the party liable for damage is generally the operator. [290] In the case of autonomous drones, the operator would be the person or entity that, although not remotely or manually steering it, has control on the overall use of the drone. The injured person would therefore have a strict liability claim against the operator if the national law stipulating the liability for aircraft accidents is considered as covering drones. Autonomous features of the drones should not have an impact on the likelihood of success of the victim's claim against the drone operator under strict liability air traffic legislation. The victim should only prove that the damage was caused by the drone without having to substantiate what made the drone fall down or drop the package.[291]

The victim could also have a claim against the operator under general national tort law rules which would require a fault of the operator. Such a fault could be envisaged for example when the drone operated under dangerous weather conditions or when the required maintenance was not performed. Depending on the provisions of national law that is applicable and to the extent the operation of the drone relies on third party service providers (for instance, the provider of GPS mapping, the provider of weather data, etc.) the operator could under certain conditions also be responsible if the accident was caused by malfunctioning of the services provided by the third party.

The victim may also sue the manufacturer under the national law provisions implementing the Product Liability Directive.[292] This would require to demonstrate a defect of the drone and to prove that the damage was caused by that defect.

---

[289] The notion of unmanned aircraft is defined in Article 3 of the Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council (2016/0277 (COD)) ('Proposal for a new Basic Regulation in the field of aviation safety').

[290] Steer Davies Gleeve, Study on the Third-Party Liability and Insurance Requirements of Remotely Piloted Aircraft Systems, Final Report, November 2014. Available at: https://www.eurocontrol.int/sites/default/files/ec_rpas_final_report_nov14_steer_davies.pdf.

[291] However, this might not be the case in jurisdictions where a fault-based liability regime applies.

[292] In a situation where the damaged property is not intended for private use, the Product Liability Directive would not apply.

As the accident of the drone may be a result of a rather large set of unknown circumstances, for instance a defect of the device, exceptional weather conditions or other circumstances such as a cyber-attacker, it will be difficult for the victim to prove the elements of a liability claim.

In most national regimes, a strict liability claim against the operator of the parcel delivery drone exists, and this appears to be an efficient way for the victim to achieve compensation.[293] In the case the operator has compensated the victim and the accident was caused by a defect of the drone or a breach of the obligations of a service provider, the operator could seek redress against the manufacturer or the service provider. If the operation of the parcel delivery drone is subject to (mandatory) insurance coverage, any potential redress claim could under statutory law be transferred to the insurance.

For example, an autonomous drone crashed into a crane in the UK in June 2017[294]. The data programmed into the drone did not include information about the crane which was erected after the programming.

Autonomous cars

Autonomous cars are motor vehicles equipped with systems that allow operating the vehicle without human intervention either partially, or completely (full automation). Autonomous cars are at present one of the most important AI applications. Their announced benefits range from a dramatic drop in the number of road accidents[295] to reduced travelling time, improved traffic flow and environmental benefits.

In the case of partial, conditional automation[296], the car operates under the supervision of the driver, but without human input under specific conditions only (for instance on certain road types or in specific geographic areas). Outside these limited environments, the vehicle requires the control by a human driver or, if the driver does not take control, it may enter into a safe fall-back mode (for instance, park the vehicle). In these cases, the driver has the responsibility to supervise the car and stand ready to re-take control if needed or upon notice. In case of higher levels of automation, the vehicle is capable to operate without any human intervention and with full automation also on any road and in any conditions. There might not even be a human person inside the vehicle and the car might not even be equipped with a steering wheel or pedals.

At the current stage, only few jurisdictions have adopted rules specifically targeting highly automated or fully automated vehicles. As a consequence, the key components of the liability regime for automated vehicles are the national civil liability rules applicable to motor vehicles.

However, under the Motor Insurance Directive[297] all Member States have to ensure that civil liability for the use of vehicles is covered by insurance and that victims of an accident caused by a

[293] A strict-liability regime of aircraft operators may not however exist in every Member State.
[294] AAIB investigation to Quest Q-200 (UAS, registration n/a), Collision with a crane, Hinkley Point, Somerset, 12 July 2017. Available at: http://www.gov.uk/aaib-reports/aaib-investigation-to-quest-q-200-uas-none.
[295] According to the World Health Organization, every year over 1.2 million people die as a result of car accidents. It is considered that 90% of accidents each year are caused by human error.
[296] SAE International's On-Road Automated Vehicle Standards Committee published the SAE Information Report: (J3016) "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems". The SAE table summarizing the different levels of driving automation defines "conditional automation" (level 3) the situation in which the automated driving system performs all aspects of the dynamic driving task with the expectation that the human driver responds adequately to a request to intervene ("fallback performance"). Available at: https://en.wikipedia.org/wiki/Autonomous_car.
[297] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability. This is a minimum harmonisation Directive, so Member States may apply higher levels of protection such as obligatory amounts of insurance cover.

vehicle enjoy a direct claim against the insurer covering the person responsible against civil liability. Although the Motor Insurance Directive does not harmonise issues of civil liability, it aims to ensure an effective protection of victims irrespective of the allocation of liability according to the different national civil liability systems.

In case of an accident caused by a fully automated vehicle, liability for a damage may be allocated to the driver/holder of the vehicle under civil law liability rules or to the manufacturer of the automated vehicle under the rules implementing the Product Liability Directive.

Practically, all Member States attribute liability for damages caused by motor vehicles to the holder or the driver of the vehicle. Liability is either fault-based, including cases where the fault can be presumed unless the holder/driver proves the opposite, or risk-based, where the holder/driver is strictly liable for having opened the risk associated with the circulation of a motor vehicle on public streets. In particular, the liability of the holder of the car is typically risk-based.

If the victim claims damages against the holder of a motor vehicle based on strict liability rules, normally there is no need to demonstrate whether the accident was caused by a wrongdoing of the car driver or another person or by any deficiency of the car. If the victim decides to pursue a claim against the manufacturer of the car based on national legislation implementing the Product Liability Directive, he has to identify and prove a defect of the car and the causal link between the defect and the damage. Considerations similar to those made in the previous case study regarding the need for the victim to prove the cause of the damage apply.

As there is mandatory insurance coverage for the use of motor vehicles under the Motor Insurance Directive and victims of accidents with insured vehicles can approach insurers directly to receive compensation, the damages will usually be paid by the insurer. In situations where an accident occurred due to a defect of a vehicle which falls under the Product Liability Directive, the victim could also have a claim against the producer of the vehicle under the law implementing the Product Liability Directive. In this context, national law could provide for redress possibilities of the insurer who compensated the victim against the producer of the defective vehicle.

Tesla: On May 7, 2016, a semi-automated Tesla Model S struck and passed beneath a truck. At the time of the collision, the truck was making a left turn and impact with the right side of the semitrailer sheared off the roof of the Tesla. The driver of the Tesla died in the crash. System performance data downloaded from the Tesla revealed that the driver was operating the car using automated vehicle control systems: Traffic-Aware Cruise Control and Autosteer lane keeping systems. The investigations revealed that although the autopilot functioned as designed, it did not detect the truck. The truck was cutting across the car's path instead of driving directly in front of it, which the radar is better at detecting, and the camera-based system was not trained to recognize the flat slab of a truck's side as a threat. The Tesla driver's lack of responsiveness indicated overreliance on automation and the monitoring steering wheel torque was not an effective method of ensuring driver engagement. The competent authority concluded that the crash was not the result of any specific defect in the autopilot system, thus Tesla was not found responsible for the accident. The competent authority noted that Tesla did an adequate job warning its customers that the autopilot system demands their supervision that their hands should remain on the wheel and their eyes on the road. The Terms of Services of the Tesla car included in cause provisions which were clarifying the semi-autonomous nature of the autopilot and were requiring the driver to take over the control of the car in 4 seconds, if the driver noticed things were not going in the right direction. Since that accident, Tesla has changed the Autopilot system so that, if a driver repeatedly ignores the Autopilot warnings, the system will stop functioning and will be prevented from restarting for the duration of the trip. If the driver never responds, the car will gradually slow down until it stops and the flashing hazard lights will come on.

Google car: On February 14, 2016, a Google self-driving car attempted to pass a municipal bus in Mountain View, California. The bus did not behave as the autonomous car predicted, and the self-

driving car crashed into it, while attempting to move back into its lane. The Google car was traveling at the stately speed of 2 mph, and there were no injuries. Google released a statement accepting fault and announcing that it was tweaking its software to avoid this type of collision in the future.

Uber car: On March 19, 2018 a woman in the street in Arizona died when hit by an autonomous Uber car, in what appears to be the first reported fatal crash involving a self-driving vehicle and a pedestrian in the US[298]. Local police reported the self-driving car was in autonomous mode at the time of the crash and that the vehicle hit a woman, who was walking outside of the crosswalk and later died at a hospital. There was a vehicle operator inside the car at the time of the crash. The circumstances of this accident had not been clarified at the moment of drafting of this Staff Working Document.

4.3 Internet of Things

Smart home ecosystem

Smart home ecosystems may include appliances, such as smart smoke detectors, smart fridges, smart thermostats, which are connected to the internet and to each other and have the ability to collect information and communicate with each other and with other systems and humans. Their operation relies on various sources of data, such as embedded sensors that automatically measure e.g. environmental parameters or monitor activity and transfer data to databases in an autonomous way, without human intervention. The data are accessed, processed and analysed by applications, which transfer commands to the physical devices in the smart home ecosystem. The various components in this ecosystem (devices, sensors, applications, etc.) may be provided by different suppliers.

For example, a smart smoke detector can be produced by manufacturer A and sold to the homeowner by seller B, a smart thermostat can be produced by manufacturer C and sold to the homeowner by seller D, the data analysis application could be provided by provider E or by one of the manufacturers of the smart appliances and the connectivity dimension is provided by internet provider F. The smart smoke detector can detect a source of fire and alert the homeowner or the fire department. In addition, the smoke detector can also communicate with other smart home appliances in the ecosystem, such as smart doors, instructing them to unlock in order to allow access to the fire fighters.

In case of a fire, not sending an alert to the fire department may ultimately result in the destruction of the house and/or damage to a neighbour's house. This may be due to various causes: a malfunctioning of the smoke detector, a faulty data processing by the application, a failure of electronic communication services or an autonomous decision to switch off the smoke detector, e.g. because of high energy consumption levels of the smoke detector. The more sophisticated an ecosystem gets, the more difficult it may be for the home owner to trace back any upcoming problem to its origin.

The home owner could have a contractual claim for damages against the seller of the thermostat or the seller of the smoke detector. This would require that the thermostat or the smoke detector were not in conformity with the sales contract. As the decision to switch off the smoke detector was taken by the application autonomously, a contractual liability of the seller of the smoke detector could be established on the basis that the device had to be designed in a way not to allow

[298] The Guardian, Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian, 19 March 2018. Available at: http://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe.

a third-party application to switch it off. The application provider would, in general, be contractually liable for the application's harmful decision.

Any claim of the home owner or the neighbour, who suffered damages from the fire, against the manufacturer of the smoke detector or the thermostat under the Product Liability Directive could be established on the basis of a defect of the device. In the above case, the consumer would have to prove the defect, more precisely which part of the smart home ecosystem was not working properly.

The neighbour could probably as well have a claim against the home owner under national tort law. This would require, in general, to prove a wrongdoing of the home owner.

If the home owner has taken out fire insurance, the insurance will probably cover the damage caused by the fire. In turn, any claim for damages which the home owner might have against the person responsible for the fire will be transferred to the insurance. In case of a complex ecosystem, the insurance faces comparable difficulties in identifying the cause for the fire and the responsible actor than the home owner.

Cyber-attacks

Internet of Things (IoT) devices may also constitute targets of cyber-attacks. In the case of smart home devices, poor security measures at design, manufacturing or operation stage may allow cyber-attackers to take control of the device and modify its functioning or the functioning of other smart devices in the same ecosystem.

In the absence of a contractual relationship to cater for cyber-attack damages, courts could impose tort liabilities on businesses (e.g. manufacturers, vendors, etc.) for the harm that a cyber-attack causes to third parties.

If we apply product liability rules to cyber-attack examples, the notions of defect, the level of safety that users are generally "entitled to expect" and the impact of software updates and functionality revisions on the safety of the product are difficult to define. Is a product defective simply because it has no update capabilities? Should the notion of defect include also a security objective, on top of the safety one?

The Product Liability Directive exempts the producer from liabilities if the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered. This exemption may as well be triggered by the manufacturer in a cyber-attack context to justify that at the moment of placing the good on the market no software vulnerability was discovered.

For example, the recent WannaCry ransomware[299] spread throughout the Internet and affected Windows-based computer systems that were running on outdated software. As well, the Mirai virus botnet leading to Distributed-Denial-of-Service attacks (on 21 October) remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US[300]. These attacks caused disruptions in various places, including hospitals, businesses, and universities resulting in multiple types of damages from destruction (or loss) of data, system downtime, lost productivity, disruption to the normal course of business, forensic investigation, restoration and deletion of hostage data and systems, reputational harm, etc. A stream of (potential) extra-contractual and contractual liability could

[299] CSO online, What is WannaCry ransomware, how does it infect, and who was responsible?, 27 September. Available at: http://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

[300] The Guardian, DDoS attack that disrupted internet was largest of its kind in history, experts say, 26 October 2016. Available at: http://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

flow from the attack with various parties to blame for it: the programmers of the malware and the attackers' group; potentially the users who failed to install the Windows security patch as the vulnerability was discovered and the patch announced, and the software vendor, which supplied the insecure code in the first place. It is unclear how liability would be allocated (if at all) between such parties in the absence of a specific regime (e.g. the duty to ensure the protection of personal data; the duty to ensure a specific level of safety or (cyber) security resilience.)[301] Most evidently, the attacker would be liable, but most of such cyberattacks are anonymous and it is difficult if not impossible for the victim to identify the attacker(s) and obtain any compensation from them. Particular users (including businesses) that failed to install the Windows security patch could also potentially face legal actions (not limited to civil actions) for the negligent failure to deliver services following the attack. In addition, contractual liability may not apply since standard terms of service frequently do not contain any promise of (cyber) security resilience. On the contrary, vendors, and especially software vendors, typically attempt to minimize or even exclude their civil liability by inserting warranty disclaimers and limitations of liability in their terms of service. That said, it is questionable whether such limitations of liability would be upheld in case of litigation in the event of a cyber-attack, since liability limitations may be deemed null and void in the case of gross negligence.

5. Questions for further analysis

5.1 Product Liability Directive

The Product Liability Directive has provided the EU liability framework for products since 1985. Since its adoption, it has accompanied many technological evolutions remaining a relevant and useful liability framework ensuring legal certainty for all parties involved. In particular, products today already include features relevant to emerging digital technologies, such as embedded software as a component of the product or connectivity elements, and have so far been adequately covered by the Product Liability Directive.

The Commission has carried out an evaluation of the Product Liability Directive[302] with a specific focus on its continued effectiveness and relevance for emerging digital technologies. The evaluation process included a preliminary assessment of the continued relevance of the Product Liability's concepts, such as product, producer, defect, damage and the burden of proof. The evaluation results as well as the forthcoming Fifth Report on the application of the product Liability Directive highlight that the Directive continues - to some extent - to be adequate for the current state of technological developments.[303]

The Directive defines **products** as movable items. Even though most producers consulted during the evaluation claimed that they did not encounter problems in distinguishing products from services so far, a number of open questions were identified related to software be it embedded or non-embedded, that will have to be further explored.

Concerning the concept of **producer**, the question arises to what extent the producer maintains control over the features of a product in the context of emerging digital technologies and can

[301] Studer, Evelyne and de Werra, Jacques, Regulating Cybersecurity - What Civil Liability in Case of Cyber-Attacks?, 19 August 2017. Expert Focus 8/2017, 511-517. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022522.

[302] Forthcoming Commission Staff Working Document on Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[303] Forthcoming Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC).

therefore be held liable for them. While in many cases the final product and producer may be easy to identify, regardless of whether it includes software or other digital elements, or whether different manufacturers have been involved in the production process, other cases may be less straightforward.

The notions of **defectiveness and burden of proof** of the Directive are fairly wide and refer to the safety levels that a consumer is entitled to expect. The defectiveness must be assessed based on an objective analysis of the expectations of an average consumer rather than on subjective expectations or predisposition of one person. The defectiveness of a product is assessed on a case-by-case basis, considering all the relevant circumstances, on the basis of objective criteria, including especially product safety legislation, and all other circumstances, including the presentation of the product, the reasonably expected use and the time when the product was put into circulation. In the context of the emerging digital technologies, it may be difficult to identify whether the damage has been caused by the product itself or by other elements interconnected to it in a digital ecosystem. In this respect, it will be necessary to provide for adequate safety levels for all types of products, taking also account of any new risks that may be posed regarding the emerging digital technologies.

At present, **damages** are limited to either physical or material damages to property that is intended for private use. While this distinction between private and professional use has not appeared to cause major problems in practice, some stakeholders have raised questions as to the continued relevance of this distinction in this day and age. Furthermore, issues related to the infringement of privacy and cybersecurity were also raised.

Finally, the exemptions, notably the **development risk clause** and the **500€ threshold** were contested by some stakeholders and will require further analysis in light of emerging digital technologies.

Thus, while a strict liability regime for producers is uncontested at EU level, the precise effects of new technological developments will have to be more closely analysed, also in light of the provisions of the Product Liability Directive, based on a better practical experience than could be gathered until now.

5.2 Broader challenges posed by emerging digital technologies

A broader and more in-depth analysis of the issues considered in this document should establish whether it is necessary and, if so, how to re-assess concepts and elements of the EU/national liability framework(s) in light of emerging digital technologies. The analysis should also include the economic dimension, including the incentives to invest on the production/provisions of these products and services and to buy them from a consumer perspective.

A first question to assess is **whether concepts like the liability of a guardian** or similar concepts **are appropriate to technologies like AI**. While AI cannot of course be assimilated to humans or animals, the autonomy element is an intrinsic feature that is relevant and very prominent in both cases. Within the limits set by relevant safety frameworks, an AI powered robot can, and actually is supposed to, act autonomously and independently, i.e. without any supervision. The approach on liability for animals is linked to the concept of lack of predictability and therefore interesting to that extent in the context of autonomous behaviour. Safety legislation will have an important role to play in reducing this unpredictability to a socially accepted minimum.

A strict liability concept which is applicable to AI systems in general does not exist. The question whether liability should be fault-based or strict for such systems is a fundamental question to explore. A reflection should be conducted on the substantive conditions for any possible liability claim, in addition to the damage suffered by the victim, for instance whether it matters if the damage could have been avoided.

While fault-based liability is generally justified by the reasoning that a wrongdoer did not respect certain requirements, for instance the reasonable standard of care, the concept of strict liability typically builds on the principle that a person who generated a risk for his own benefit should be responsible for any damage materialised in connection to that risk. Current strict liability provisions could already apply to the use of certain AI powered devices, in particular, in the case of automated cars. Another question is **whether and to what extent it matters for determining liability whether the damage could have been avoided or not**. In the specific national liability schemes regarding the collapse or ruin of buildings, the exercise of dangerous activities and the liability of the employer, any person held liable by law could avoid liability by proving that he/she did everything possible to avoid the damage or that they used reasonable care considering similar circumstances. For instance, if the owner of a building shows that he used reasonable care in the maintenance of the building, and therefore the damage was not caused by poor maintenance, he can avoid liability. By analogy, this could mean that the owner of an advanced robot could avoid liability if, for instance, he had used and maintained the robot properly, respecting the instructions of the producers and updating the software when required. However, as explained above, these technologies might in such scenarios still perform autonomous behaviour and cause damage. The damage might occur even if the use and maintenance of the robot are impeccable. Considering the autonomy aspect, this would raise the question, what actions a person held liable could possibly put in place in order to avoid the damage caused by the autonomous behaviour of emerging digital technologies.

Questions related to **cybersecurity** are also to be assessed. Security breaches, in particular through cybersecurity attacks, are certainly among the most serious risks posed by these technologies. In most cases, it is likely very difficult, if not impossible, for the victim to identify the attackers and bring a claim for damages against them, meaning that, absent holding someone else liable vis-à-vis the victim, this would likely remain without compensation. If one considers the possibility of holding the operator/owner of the device or the producer liable, such liability would be however of a very different nature. Although the risk inherent in the emerging digital technologies would have been materialised, the existence of an actual wrong-doer at the origin of the damage would have been known, but not his/her identity. If therefore such liability were to be created at all, one would have to consider -at least in such cases- to grant the operator or producer a defence if the operator/owner of the device had used all applicable standards of care and diligence for the use and maintenance/production of the device and yet the cyberattack was successful.

It is also important to assess the issue of the **burden of proof**. National regimes including fault-based liability schemes or different forms of strict liability regimes often include provisions, whereby the burden of proof for a possible fault, defect or other condition is not placed on the victim. Thus, the person held liable by law would need to prove to be discharged from liability, for instance, that the damage was caused as a result of force majeure or an act/behaviour of a third party. Whether the burden of proof should be on the claimant or reversed, what substantive conditions the claimant should demonstrate as well as the impact on the ability of the claimant to obtain compensation are important elements to assess.

The type of damage to be covered should also be assessed.[304] Which type of damage caused by these technologies should be compensated; death, bodily harm, harm to property or also consequential damages in form of purely economic damage? Non-material damage? Especially for the latter, one would also need to consider whether the damage of only natural or also of legal persons should be compensated. In this context, it would also need to be considered whether the liability for the use of AI powered devices should have a threshold and/or be capped, which

[304] The Product Liability Directive stipulates an obligation of producers to compensate natural persons for damages caused by defective products resulting from death, personal injury or damage to or destruction of an item of property. The Directive is without prejudice to national provisions relating to non-material damage.

amount(s) should be chosen and whether they should differ according to sectors. In the context of this set of questions, it would be helpful to consider the damages including non-material damages that could typically materialize in light of the risks connected with the use of AI powered systems taking into account that these technologies may create new types of risks or accentuate existing risks.

The question of **redress between actors in the value chain**[305] is an important question to be further discussed. While it is not necessarily relevant for the purpose of ensuring that the victim obtains compensation for the damages suffered - which may happen satisfactorily - the question of redress has to be considered from an overall policy standpoint, particularly in situations where a complex ecosystem of market operators enables the roll-out and functioning of the emerging digital technologies. The redress is indeed crucial for the roll-out emerging digital technologies as the value chain of these technologies present a degree of complexity that is higher than that of other value chains and it will answer the question of who ultimately bears the cost for possible damages. If, for instance, the owner or operator of an AI system is considered strictly liable, even if he has no possibility to control its behaviour or to prevent any associated risks with the adoption of precautionary measures, he should be able to obtain redress for the damages covered, to the extent that the wrongful or undesirable behaviour of the AI system may be attributable to someone else, e.g. the producer. However, this might prove challenging. Although the person held liable under national law does not have to prove the fault of the producer under the Product Liability Directive, this person would still have to prove the defect and the causal link between the defect and the damage.

Conceptually speaking, a strict liability approach to AI powered devices would acknowledge that damages resulting from the use of these devices cannot entirely be avoided. At the same time, it would ensure that potential victims are compensated by the liable person, regardless of any wrongdoing. In order to facilitate the victim's compensation and protecting the victim from the risk of insolvency of the liable person, it could be discussed, among other solutions, whether various actors in the value chain should be required to take out insurance coverage as it is the case today for cars. In case of an accident, the victim would be compensated by the insurance. On their end, although they may still face important difficulties due to the complexity of the technology, insurance companies could use their expertise and assets to assess whether a redress claim against the manufacturer of the AI powered device or any other person can be enforced.

6. Next steps

The Commission will analyse the above liability questions with the help of the Expert Group on liability, which will consist of two formations: the Product Liability Directive formation and the New Technologies formation.[306] At the same time, it is important to continue analysing what could or should be done to prevent possible damages through an appropriate safety framework.

In the context of the work of the Product Liability Directive formation, questions to be discussed relate, for example, to an update of the concepts of 'producer', 'product' and 'defect', the exemptions and other elements of the Directive, in order to reflect the technological and other developments in the single market and global value chains.

In the context of the analysis of the overall liability regimes and approaches that are or can be relevant to the goal of facilitating the uptake of emerging digital technologies by fostering investment stability and users' trust, the New Technologies formation will analyse other relevant issues, for instance those covered in Section 4.2.

---

[305] Actors in the value chain may include producers, service operators, software providers, traders, conformity assessment bodies and infrastructure providers.

[306] Call for experts for a group on liability and new technologies. Available at: https://ec.europa.eu/digital-single-market/en/news/call-experts-group-liability-and-new-technologies.

The approaches put forward by the "Building a European Data Economy" Communication based on initial input from stakeholders should also be considered.

If a regulatory intervention on these technologies appears appropriate and necessary (in terms of new rules or an amendment to existing rules), it should be discussed whether that intervention should be developed **in a horizontal or sectorial way and whether new legislation should be enacted at EU level.**

ANNEX I – Specific Characteristics of Emerging Digital Technologies

This annex describes the specific characteristics of the Internet of Things and Artificial Intelligence, which have been used to conduct the analysis in this document. These characteristics are shared to a certain degree by other emerging digital technologies like Blockchain, 3D Printing and cloud computing.

The Internet of Things (IoT)

The Internet of Things (IoT) is about setting up new ecosystems that cut across vertical areas, and create new markets for hardware (connected devices), software (IoT platforms and systems) and services (IoT applications). IoT has a horizontal and cross-cutting character. It should be understood as an ecosystem where areas that have been developed as vertical silos (manufacturing, transport, healthcare, devices, etc.) relate to each other, thanks to common platforms and cross-cutting innovation. IoT ecosystems are, therefore, based on bringing together multiple sectors and a variety of stakeholders to cover an increasingly complex value chain.

IoT is based on various disciplines and technologies like sensors, embedded systems, various communications technologies. It requires a specific configuration for object identification and search, open/closed data sharing, lightweight communication protocols, trade-off between local and networked based information processing, and back-end integration. It also requires specific considerations of data security (e.g. location-based profiling), liability (many service providers involved), seamless identification and authentication mechanisms (including those of persons/entities needed for managing contractual relations, attribution and liability) and trust. All this increases the complexity of the IoT ecosystem.

Connected sensors in private, business or city environments collect data from objects (e.g. a car, a phone, etc.) and these data are analysed either through embedded systems or through cloud-based and Internet systems enabling the creation of new services based on big data analytics.

The data provided by connected sensors and objects allow single and networked objects to take decisions based on the data and actuate or perform specific functions derived from sensing, analysis and intelligence gathered. This takes place normally within the boundaries of given applications but it is expected, with increasing computing power and sophistication, to gain high levels of autonomy in their behaviour and “life”. Examples include factory automation, logistics and robotics.

But sensors and smart connected objects are not only designed and optimised to perform certain functions on the basis of vertical business models. They become part of a bigger connectivity network which creates new opportunities to combine more intelligence and actuation across vertical markets and to provide a whole new set of services. Technical and semantic interoperability are the key factor of success. It enables the programming of complex systems to integrate a number of device- and service-providers to deliver complete IoT solutions e.g. at home, in cities, between industries.

Therefore, IoT demonstrates the following specific characteristics:

- Complexity: Given the numerous interdependencies in the value chain and the variety of actors;
- Autonomous behaviour: Many of the operations provided through and by an IoT system can be fully autonomous;
- Data driven: It entails data generation, data gathering, data processing and data analysis;
- Openness due to its digital dimension encompassing tangible and intangible elements (software and data).

In light of these characteristics, it can be concluded that IoT encompasses all of the main specificities that revolve around these technologies: high levels of complexity and high interdependency, the element of autonomy, data generating and/or processing components, and an open dimension.

Artificial Intelligence (AI)

Artificial intelligence (AI) aims to study and develop intelligent machines and software. The associated ICT research includes the development of software that can reason, gather knowledge, plan intelligently, learn, communicate, perceive, and manipulate objects.

AI is used in a variety of ways and can be found across a large number of sectors, from assembly line robots to advanced toys, and from speech recognition systems to medical research. Its most common application is to find patterns in data, which is why it is commonly applied in online search engines and recommendation sites. Another common application is advanced robotics.

AI can allow users of big data to automate and enhance complex descriptive and predictive analytical tasks that would be extremely labour intensive and time consuming, if performed by humans. Unleashing AI on big data can have a significant impact on the role data plays in deciding how we work, how we travel and how we conduct business. More and more aspects of our lives can become predictable, from travel time to customer satisfaction to how long it will take an abled bodied worker to complete a given task.

Also, AI can provide this type of information ahead of time, allowing for improved planning, scheduling, and decision making, providing users with critical information at the right time to make the best opportunities when they present themselves. Moreover, tying the use of artificial intelligence on big data to responsively designed user applications allows for improved user experience that benefits from receiving the required information based on interaction context, without swiping, pinching, scrolling or clicking.

Therefore, we can see that AI combines certain specific characteristics such as:

- Complexity: with machine learning, AI can learn from other AI.
- Autonomous behaviour: Depending on the application, AI software can reason, gather knowledge, plan intelligently, learn, communicate, perceive, and manipulate objects.
- Data driven: AI entails data gathering, data processing and data analysis;
- Openness: AI combined with hardware can create new tangible products and/or deliver services.

ANNEX II – List of EU Legislation

1. Council Directive 70/157/EEC of 6 February 1970 on the approximation of the laws of the Member States relating to the permissible sound level and the exhaust system of motor vehicles (OJ L 042 , 23.02.1970, p. 16-20);

2. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29–33);

3. Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (OJ L 183, 29.06.1989, p. 1-8);

4. Council Directive 92/42/EEC of 21 May 1992 on efficiency requirements for new hot-water boilers fired with liquid or gaseous fuels (OJ L 167, 22.6.1992, p. 17–28);

5. Directive 2000/14/EC of the European Parliament and of the Council of 8 May 2000 on the approximation of the laws of the Member States relating to the noise emission in the environment by equipment for use outdoors (OJ L 162, 3.7.2000, p. 1–78);

6. Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 011, 15.01.2002, p. 4-17);

7. Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26–42);

8. Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community (OJ L 200, 7.6.2004, p. 50–57);

9. Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26–42);

10. Directive 2005/64/EC of the European Parliament and of the Council of 26 October 2005 on the type-approval of motor vehicles with regard to their reusability, recyclability and recoverability and amending Council Directive 70/156/EEC (OJ L 310, 25.11.2005, p. 10–27);

11. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery (OJ L 157, 9.6.2006, p. 24–86);

12. Directive 2006/40/EC of the European Parliament and of the Council of 17 May 2006 relating to emissions from air conditioning systems in motor vehicles and amending Council Directive 70/156/EEC (OJ L 161, 14.6.2006, p. 12–18);

13. Directive 2006/66/EC of the European Parliament and of the Council of 6 September 2006 on batteries and accumulators and waste batteries and accumulators and repealing Directive 91/157/EEC (OJ L 266, 26.9.2006, p. 1–14);

14. Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and

commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (OJ L 171, 29.6.2007, p. 1–16);

15. Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (OJ L 263, 9.10.2007, p. 1–160);

16. Directive 2008/2/EC of the European Parliament and of the Council of 15 January 2008 on the field of vision and windscreen wipers for wheeled agricultural or forestry tractors (Codified version) (OJ L 24, 29.1.2008, p. 30–38);

17. Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005 (OJ L 141, 31.5.2008, p. 5–10);

18. Regulation (EC) No 78/2009 of the European Parliament and of the Council of 14 January 2009 on the type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users, amending Directive 2007/46/EC and repealing Directives 2003/102/EC and 2005/66/EC (OJ L 35, 4.2.2009, p. 1–31);

19. Regulation (EC) No 79/2009 of the European Parliament and of the Council of 14 January 2009 on type-approval of hydrogen-powered motor vehicles, and amending Directive 2007/46/EC (OJ L 35, 4.2.2009, p. 32–46);

20. Directive 2009/20/EC of the European Parliament and of the Council of 23 April 2009 on the insurance of ship-owners for maritime claims (OJ L 131, 28.5.2009, p. 128–131);

21. Directive 2009/34/EC of the European Parliament and of the Council of 23 April 2009 relating to common provisions for both measuring instruments and methods of metrological control (OJ L 106, 28.4.2009, p. 7–24);

22. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1–37);

23. Regulation (EC) No 392/2009 of the European Parliament and of the Council of 23 April 2009 on the liability of carriers of passengers by sea in the event of accidents (OJ L 131, 28.5.2009, p. 24–46);

24. Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC (OJ L 188, 18.7.2009, p. 1–13);

25. Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their

trailers and systems, components and separate technical units intended therefor (OJ L 200, 31.7.2009, p. 1–24);

26. Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity (OJ L211, 14.08.2009, p.55-93), to be repealed by the outcome of negotiations of the Commission Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast / COM/2016/0864 final/2 - 2016/0380 (COD);

27. Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (OJ L 263, 7.10.2009, p. 11–31);

28. Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of eco-design requirements for energy-related products (OJ L 285, 31.10.2009, p. 10–35);

29. Implementing acts to the Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of eco-design requirements for energy-related products (OJ L 285, 31.10.2009, p. 10–35);

30. Regulation (EC) No 1005/2009 of the European Parliament and of the Council of 16 September 2009 on substances that deplete the ozone layer (OJ L 286, 31.10.2009, p. 1–30);

31. Directive 2010/31/EU of the European Parliament and of the Council of 19 May 2010 on the energy performance of buildings (OJ L 153, 18.6.2010, p.13-35);

32. Directive 2010/35/EU of the European Parliament and of the Council of 16 June 2010 on transportable pressure equipment (OJ L 165, 30.6.2010, p. 1–18);

33. Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1–13);

34. 2012/23/EU: Council Decision of 12 December 2011 concerning the accession of the European Union to the Protocol of 2002 to the Athens Convention relating to the Carriage of Passengers and their Luggage by Sea, 1974, as regards Articles 10 and 11 thereof (OJ L 8, 12.1.2012, p. 13–16);

35. Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC (OJ L 315, 14.11.2012, p. 1–56);
36. Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1–51);

37. Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52–128);

38. Directive 2013/29/EU of the European Parliament and of the Council of 12 June 2013 on the harmonisation of the laws of the Member States relating to the making available on the market of pyrotechnic articles (OJ L 178, 28.6.2013, p. 27–65);

39. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90–131);

40. Commission Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall (OJ L 91, 3.4.2013, p. 1–4);

41. Directive 2014/28/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses (OJ L 96, 29.3.2014, p. 1–44);

42. Directive 2014/29/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of simple pressure vessels (OJ L 96, 29.3.2014, p. 45–78);

43. Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (OJ L 96, 29.3.2014, p. 79–106);

44. Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments (OJ L 96, 29.3.2014, p. 107–148);

45. Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (OJ L 96, 29.3.2014, p. 149–250);

46. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251–308);

47. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309–356);

48. Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits (OJ L 96, 29.3.2014, p. 357–374);

49. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62–106);

50. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment (OJ L 189, 27.6.2014, p. 164–259);

51. Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146–185);

52. Regulation (EU) No 517/2014 of the European Parliament and of the Council of 16 April 2014 on fluorinated greenhouse gases and repealing Regulation (EC) No 842/2006 (OJ L 150, 20.5.2014, p. 195–230);

53. Regulation (EU) No 540/2014 of the European Parliament and of the Council of 16 April 2014 on the sound level of motor vehicles and of replacement silencing systems, and amending Directive 2007/46/EC and repealing Directive 70/157/EEC (OJ L 158, 27.5.2014, p. 131–195);

54. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1–50);

55. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51–98);

56. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99–147);

57. Directive (EU) 2016/798 of the European Parliament and the Council of 11 May 2016 on railway safety (OJ L 138, 26.5.2016, p. 102–149);

58. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44–101);

59. Council Directive of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (90/385/EEC) (OJ L 189, 20.7.1990, p.17);

60. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p.1);

61. Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices (OJ L 331, 7.12.1998, p. 1);

62. Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (OJ L 198, 28.7.2017, p. 1–23);

63. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88);

64. Delegated acts to the Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (OJ L 198, 28.7.2017, p. 1–23).

List of other relevant non-legislative texts concerning artificial intelligence in the European Union

European Comission. ***Liability for Artificial Intelligence and other emerging digital technologies*****. Expert Group on Liability and New Technologies - New Technologies Formation, 2019.**

European Parliament. ***Artificial Intelligence and Civil Liability*****. A study requsted by the Policy Department C at the request of the Committee on Legal Affairs, 2020.**

European Comission. ***Ethics Guidelines for Trusthworthy AI.*** **High-Level Expert Group on Artificial Intelligence, 2019.**

Working document on the free flow of data and emerging issues of the European data economy

Comission Staff working document on the free flow of data and emerging issues of the European data economy accompanying the Communicaton "Building a European Data Economy" {(COM/2017) 9 final)}

Part 1: Context and purpose of this document

A thriving data-driven economy is essential for innovation, growth, jobs and European competitiveness as well as for a functional Digital Single Market. The Communication "Towards a data-driven economy"[307] presents a vision for the data-driven economy as an ecosystem with different types of players (e.g. data providers, data analytics companies, skilled data and software professionals, cloud service providers, companies from the user industries, venture capitalists, entrepreneurs, public services, research institutes and universities), leading to more business opportunities, in particular for SMEs. The availability of good quality, reliable and interoperable datasets was specifically highlighted as an important enabler for new data products.

Building on this, the Digital Single Market strategy[308] outlined a set of concrete actions to address existing barriers to the free flow of data across borders and sectors. It emphasised the commitment of the EU to the highest standards of protection of personal data. In this respect it expressed the view that the General Data Protection Regulation (GDPR) – still under discussion at the time – would increase trust in digital services through the protection it would offer to individuals with respect to the processing of their personal data. Subsequently, the GDPR was adopted. It constitutes a comprehensive and complete framework with respect to processing of personal data.

The Communication "Building a European Data Economy" that this Staff Working Document accompanies suggests that Europe is not tapping into the potential of data for business, research and innovation purposes. In this document, the Commission sets out the policy context and a first analysis of the problem drivers on these emerging issues together with a non-exhaustive list of broad principles that could help shaping an EU framework for the free flow of data and improved sharing of commercial data and in particular machine-generated data which are either non-personal in nature or personal data that have been anonymised.

The purpose of this Staff Working Document is to provide additional evidence and a detailed description of the emerging issues relevant for the EU data economy. The objective is to inform the debate and in particular the stakeholder consultation announced in the Communication. It builds on preliminary available evidence and a first set of stakeholder consultation meetings.

[307] COM(2014)442 final of 2 July 2014.
[308] COM(2015)192 final of 6 May 2015.

Part 3: Data Access and Transfer

(…)

6. Rights on data and access to data in specific sectors

6.1 Data from connected vehicles

Access to and re-use of non-personal or anonymised data have been subject to intensive discussions with respect to data generated by the "smart" and connected car.

Building on existing legislation providing for access to in-vehicle information for the purposes of ensuring a level playing field on the after-sales repair and maintenance market[309], and preparing for a legislative initiative on "an interoperable, standardised, secure and open-access platform"[310], the issue of access to in-vehicle data has been discussed in depth since 2014, in the framework of a C-ITS stakeholder platform.[311] Five guiding principles for access to in-vehicle data and resources have been agreed upon, including fair and undistorted competition and the importance of "standardised access" to in-vehicle data as an enabler of the "common use" of such data in the context of the "data economy".[312] Work is on-going in terms of evaluating the technical and legal feasibility of improving access to in-vehicle data.[313]

(…)

Part 4: Liability

Based on the emergence of Big Data we have witnessed the rapid development of new technologies and, as a consequence, of sophisticated data-based products and services coming out from emerging technologies like Internet of Things (IoT) and Cloud Computing. Technological progress has contributed to the expansion and increased use of Artificial Intelligence (AI), allowing different autonomous systems applications (e.g. robots) to be deployed and used in numerous contexts, from industrial purposes to private uses.

One significant element in the operation of these emerging data based products and services are the highly complex interdependencies which are being formed between their different layers: the data layer (collection and processing), the software layer (whether embedded or not), the applications layer encompassing different apps, sensors and actuators, data services and/or tangible/ connected/ automated systems[314] devices, as well as the connectivity layer, such as the network connectivity, the data platforms and the digital infrastructures.

---

[309] Regulation 715/2007 as amended.
[310] Article 12(2) Regulation (EU) 2015/758 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, OJ L 123 of 19/05/2015, p. 77; the deadline for adopting a legislative proposal is 9 June 2017.
[311] http://ec.europa.eu/transport/themes/its/c-its_en.
[312] See C-ITS platform final report, January 2016, http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf, p. 11-12.
[313] Follow-up supporting study on 'Interfaces for access to services and vehicle resources' (open in-vehicle platform), 2015/S 248-450626 (ongoing).
[314] E.g. smart fridges, robots, drones, automated cars etc.

When damage occurs in the context of the use of such technologies, legal challenges may arise in relation to assigning liability, as well as in relation to product compliance, safety and insurance-related aspects.

Liability is defined in relation to a damage caused to another person. A liability regime defines the (natural or legal person) responsible in case damage is caused to another person and the conditions under which the latter can exercise its liability claims.

Contractual liability can be derived from the violation of the terms of the contract or statutory contract law rules.

Extra-contractual liability relates to the civil law responsibility for damage which caused outside the context of a contract (the damage being caused by a violation of a right or legitimate interest protected by law).

Product liability is a form of extra-contractual liability referring to the civil liability of manufacturers; at EU level this was introduced by the Directive on Defective Products Liability (85/374/CEE). This Directive establishes a strict liability, i.e. where a defective product causes damage to a consumer, the producer may be liable even without negligence or fault on his part.

Under this Directive, a product is considered to be defective where it does not provide the safety which a person is entitled to expect, taking all circumstances into account[315]. The injured person carries the burden of proof having to demonstrate the actual damage, the defect in the product, and a causal link between the damage and the defect.

1. The new environment for liability in the digital economy

1.1 The Internet of Things (IoT)

Liability in relation to IoT products and services has been identified as a specific issue to be tackled as part of the Digital Single Market Strategy. A first analysis of liability and safety issues arising in relation to IoT products and services can be found in the recently published Staff Working Document "Advancing the Internet of Things in Europe"[316].

IoT is a wide-ranging ecosystem of physical objects connected to the Internet, capable of identifying themselves and communicating data to other objects with the help of a communication network for digital processing.

It is assumed that new market players will enter the chain of liability, both in relation to data gathered through IoT technologies, and in relation to any possible damage that may be caused by IoT devices introduced on the market and the related-services which are respectively being provided. Indeed, any IoT product/service is highly dependent on the quality and timeliness of the data which it receives and that are processed for various decision-making processes.

But the quality and accuracy of data are only one aspect in relation to the liability challenges that the IoT and autonomous systems raise. Thus, one of the most significant challenges for determining liability is the fact that the IoT ecosystem involves a wide range of market players which are each providing different parts and layers of this ecosystem. These different IoT layers encompass tangible elements (e.g. the hardware, products), the embedded software, the provision of software maintenance services, the supply of digital infrastructures as well as the processing and exploitation of data. Moreover, by the nature of its design, an IoT product/service is highly dependent on third party technologies to perform its functions and to also maximise the benefit to the user.

---

[315] Including the presentation of the product, the reasonable use of the product, and the time when the product was put on the market.

[316] SWD(2016) 110 final, https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe.

On the one hand, the multiplicity of market players may raise liability problems for defects in relation to one single IoT device, as well between the network of IoT connected devices. For instance, in the case of a connected car, damage may be caused by problems with defects which may originate from the product manufacturer, the internet provider, from the data platform holder or the connectivity provider. In the situation where the cars are connected among themselves, problems may also come from the inter-action and data exchange flow between these different vehicles.

On the other hand, and in addition to that, when different devices are being connected to the Internet and among themselves - which is the very specificity of the IoT - the difficulty for the consumer/user in identifying with which of the different market players the cause of the problem lies is all the more greater.

For instance, smart home technology promises many benefits, especially for elderly people living alone. A smart home could notify the resident when it is time to take medicine, alert the hospital if the resident falls and track how much the resident is eating. If a person is a little forgetful, the smart home could perform different tasks, such as shutting off the water before a tub overflow or turning off the oven if the cook had forgotten that. If, for instance, a problem occurs and the water is not turned off, thus leading to a flood and damage to property, the identification of where in the ecosystem of the different IoT devices the problem occurred or proving the relationship between the defect and damage may be complicated.[317]

Another example could be a security system in a smart home which will, in case of emergency, notify the resident that the fire alarm is on, connect to the system that locks the doors, by unlocking them, and connecting to the electric network of the house lighting the path to safety, finally connecting to the telephone landline and dial the fire department. If a problem occurs and the interaction with the electric network of the house lighting is disrupted, it would be again difficult to discover whether there was for instance a problem of sensors failing to react, the data service itself being disrupted or an issue with the server connectivity.

The development of IoT technologies is therefore likely to create sophisticated interdependencies between product and service producers. These dependencies are not static. They can increase and become more complex, over the life of the product/service. They can give rise to challenges in determining where exactly the fault lies in the event of a problem. While issues relating to liability when products involve third party components are of course not new, they can be emphasised in some specific IoT applications[318] or more generally when different products are increasingly becoming connected among themselves and, for that purpose, more complex in their design and system integration features.

Any interdependency also gives rise to a number of questions such as to who is responsible for certifying the safety of the product, for ensuring the safety on an on-going basis and finally as stated before, how liability should be allocated in the event that the technology behaves in an unsafe way, causing damage.

These issues, if not properly addressed by existing legal frameworks or contractual arrangements, may result in legal uncertainty, increasing investment risks and thereby the roll-out of the Internet of Things.

It may also affect the uptake of data-driven services and products from the consumer side. Since most consumer products will tend to become ''smart' products in the future, it is fair to assume that more and more end-users will be using a rather complex product involving complex interactions with third parties, necessary for its functioning.

---

[317] In Hufford v Samsung Electronics (UK) Ltd., 148 for example, the claimant was unable to discharge the burden of proof that a fridge-freezer caused a fire in his home.

[318] The IoT agriculture market, domotics market.

Users of these new technologies may face legal uncertainty to claim damages and thus develop a lack of trust

1.2 Autonomous systems

Autonomous systems come in many different shapes and forms, ranging from classical industrial robots to self-driving cars, from highly autonomous combine harvester to unmanned underwater vehicles, from surgical robots to drones. What bind these diverse systems together is their physical embodiment and the fact that they are all capable to ''understand'' and ''interpret'' their environments and act appropriately.

Driven by technological progress in nano-electronics and low power computing, as well as by increased capabilities of the robots (such as sensing, actuating, cognitive vision and machine learning), these systems are increasingly endowed with the capacity to better perceive and interpret their environment, interact with humans, learn new behaviours and execute actions autonomously without a human in the loop.

The more autonomous these systems become, the less they can be considered simple tools in the hands of other actors (the manufacturer, the owner, the user, etc.). Autonomy has thus important legal implications insofar as the impact of such systems on their environment also triggers effects on third parties' rights and duties. The increasing degree of autonomy thus poses a challenge to the current regulatory framework as a natural or legal person needs to ultimately be held responsible for such an impact.

More autonomous decision-making may thus conflict with the current regulatory framework which was designed in the context of a more predictable, more manageable and controllable technology. Clarifying and, if necessary, adapting the legislative framework is therefore essential for both citizens to be able to trust and make the best use of this technology and as well for the European industry to be able to lead and capture the opportunities arising in this field.

In the case of autonomous systems (e.g. robots) the increasing degree of autonomy is the feature that poses most challenges to the current liability rules. The autonomous decision-making features in robots - due to ''learning'', ''understanding'' and other ''cognitive-like'' features may lead to unexpected or unintended consequences.

2. Liability challenges in relation to Internet of Things and autonomous systems

To assess challenges in this field, one should ask whether the IoT and the autonomous systems trigger conceptually new liability issues or whether they raise new challenges for managing liability.

Given that IoT and autonomous systems are fairly new/emerging markets, more and in-depth information and evidence would have to be gathered to fully assess possible issues in relation to liability in the context of the use of such technologies.

Example: Connected and automated driving

Connected cars exchange information with other cars, or with the road infrastructure or with remote data bases. This allows for provision of driving assistance or mobility services or other type of services useful for the actors part of that value chain.

In principle, in EU countries, the law is currently quite clear in the respect that registered car owners are, in the first instance, liable for accidents caused by their vehicle and required to be insured against such an eventuality in accordance with the motor insurance directive. Car owners or the insurer then might have the opportunity to pursue recourse against the vehicle manufacturer if it can be established that the accident was caused by a defect for which the manufacturer is responsible under the Defective Product Directive. This was confirmed in the

recommendations of the Commission GEAR 2030 working group on automated and connected vehicles.[319]

Cars have contained components produced by different entities for years, so that also for non-connected cars the technical determination of where the defect originated can be difficult. This is why the current liability framework attempts to reduce uncertainty by establishing liability ex ante, and in some cases with no necessity to prove fault.

But with increasing actors in the connectivity chain, the attribution of liability needs to be examined with care. Accidents could potentially be caused also by connectivity problems due to network failures under a complex bundle of physical products and services context.

In the situation of partially self-driving vehicles, technology may take over some driving responsibilities but the driver may still be required to remain in control to monitor the operation by the vehicle software. This partial shift of paradigm may already in itself be problematic as the division and interplay between the roles, and consequently the liability, of humans and that of technology still needs to be investigated in the context of self-driving vehicles.

The problem may become more acute with fully automated vehicles. With no human in control, the product as a whole and the technology in particular need to be able to behave and perform safely, for instance the software algorithms or the sensors need to be able to cater for a wide range of unexpected situations.

With sophisticated IoT and autonomous systems, it is an open question whether liability for such emerging technologies should be modelled around rules on liability for defective products.

It is not clear either whether and how traditional concepts and provisions of the current legal regime for product liability (for instance, the definitions of ' defect', 'producer', 'damage', or the rule of the burden of proof) can apply in the context of IoT and autonomous systems.

In light of the IoT and autonomous systems characteristics, as exemplified above, questions may arise in relation to concepts used in product liability regimes.

1) It is not clear how to classify the IoT/autonomous system devices, whether for instance the IoT devices could be qualified as products or as services since it is possible that distinctions used in the past may not fully capture specificities of new complex digital technologies.[320] Most product liability regimes only apply to goods, while services and goods that come with the provision of a service being excluded. The matter is left to contractual arrangements which may provide for liability exclusions. In case of legal gaps or legal uncertainty, the consumer/user may face difficulties to claim certain type of damages that these IoT/autonomous systems can generate.

2. Does the definition of defect fit with the type of defects that may arise in systems encompassing software? Can a learnt new behaviour leading to damage be considered a defect? Even without learning systems, it needs to be clarified whether an undesirable autonomous behaviour can and should be considered a defect. Does the concept of ''producer'', fit with the type of roles and responsibilities that may arise in systems encompassing software and in the data value chain?

[319] The GEAR 2030 High Level Group gathering the relevant Ministers, Commissioners and stakeholders was set up in October 2015 to make recommendations to the Commission to tackle the future challenges affecting the automotive sector by 2030. On automated and connected vehicles, the goal of the group is to present first recommendations by the end of 2016 (link here below) with final recommendations by mid-2017:
http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8640
https://circabc.europa.eu/w/browse/23eaf3be-3b5b-4b22-96a3-c4d33d254795.

[320] For example, in the IoT context, an issue is to assess to what extent the "product" can be said to include its intangible component parts, specifically the software and the data, given that in some circumstances software was legally assessed as a service and not part of the device of which it is component.

Should the producer be the right or only right addressee of liability, since as stated above, the IoT devices generally involve many different actors in the value chain which all enable the IoT technology to function (product manufacturers, software producers, the connectivity service, the sensor manufacturers, the owner of the object, service provider independent from the manufacturer/software producer etc.).

In conclusion, as far as IoT products/services are concerned, and in light of their characteristics as described above it may become difficult to localise a malfunctioning problem and consequently hold a particular market player liable if something goes wrong between multiple IoT interoperating devices.

In respect to the autonomous systems, robots may display increasing levels of autonomy and make decisions without human intervention even using in some cases degrees of artificial intelligence to perform tasks. This prompts the question whether in the case of sophisticated autonomous systems the degree of autonomy should be an important element in the legal framework.

EC services are currently evaluating the Directive on Liability for defective products. The evaluation will analyse whether the challenges of determining and allocating liability arising from the generation and processing of data based products coming out of these emerging technologies are appropriately dealt with.

Therefore, the Commission will invite stakeholders in the upcoming debate to explore the feasibility of different other approaches which may provide interesting avenues for addressing these challenges. Discussions may revolve around the following broad directions:

- A **strict liability regime**
- A liability regime based on a **risk-generating** approach. According to this principle, liability would be assigned to the actors generating a major risk for others and benefitting from the relevant device, product or service.
- A **risk-management** approach, where liability is assigned to the market actor which is best placed to minimize or avoid the realisation of the risk or to amortize the costs in relation to those risks.
- These solutions could be coupled with voluntary or mandatory insurance schemes for compensating the parties who suffered the damage. Such schemes could for instance be funded by insurance contributions made by manufacturers, software developers, as well as other relevant market players in the IoT/robotics value chain. This approach would need to build on the dual objective of both providing legal protection to investments made by business, while reassuring consumers regarding a fair compensation or an appropriate insurance in case of damage.

Finally, apart from the issues related to extra-contractual liability, further reflection may also be needed to assess whether clarification or adaptation of existing contract law rules are needed for the Machine-2-Machine contracting paradigm.

The increased use of automated auctioning systems, automated trading in stock markets, as well as, more generally of new digital technologies such as distributed ledgers technology (blockchains) deserve particular attention with a view to understand whether they raise any challenges in respect of traditional civil and contract law concepts and rules.

(…)

Recommendation for Civil Law Rules on Robotics

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))

The European Parliament,

– having regard to Article 225 of the Treaty on the Functioning of the European Union,

– having regard to Council Directive 85/374/EEC[321],

– having regard to the study on Ethical Aspects of Cyber-Physical Systems carried out on behalf of the Parliament's Science and Technology Options Assessment (STOA) Panel and managed by the Scientific Foresight Unit (STOA), European Parliamentary Research Service;

– having regard to Rules 46 and 52 of its Rules of Procedure,

– having regard to the report of the Committee on Legal Affairs and the opinions of the Committee on Transport and Tourism, the Committee on Civil Liberties, Justice and Home Affairs, the Committee on Employment and Social Affairs, the Committee on the Environment, Public Health and Food Safety, the Committee on Industry, Research and Energy and the Committee on the Internal Market and Consumer Protection (A8-0005/2017),

Introduction

A. whereas from Mary Shelley's Frankenstein's Monster to the classical myth of Pygmalion, through the story of Prague's Golem to the robot of Karel Čapek, who coined the word, people have fantasised about the possibility of building intelligent machines, more often than not androids with human features;

B. whereas now that humankind stands on the threshold of an era when ever more sophisticated robots, bots, androids and other manifestations of artificial intelligence ("AI") seem to be poised to unleash a new industrial revolution, which is likely to leave no stratum of society untouched, it is vitally important for the legislature to consider its legal and ethical implications and effects, without stifling innovation;

C. whereas there is a need to create a generally accepted definition of robot and AI that is flexible and is not hindering innovation;

D. whereas between 2010 and 2014 the average increase in sales of robots stood at 17% per year and in 2014 sales rose by 29%, the highest year-on-year increase ever, with automotive parts suppliers and the electrical/electronics industry being the main drivers of the growth; whereas annual patent filings for robotics technology have tripled over the last decade;

E. whereas, over the past 200 years employment figures had persistently increased due to the

[321] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29).

technological development; whereas the development of robotics and AI may have the potential to transform lives and work practices, raise efficiency, savings, and safety levels, provide enhanced level of services; whereas in the short to medium term robotics and AI promise to bring benefits of efficiency and savings, not only in production and commerce, but also in areas such as transport, medical care, rescue, education and farming, while making it possible to avoid exposing humans to dangerous conditions, such as those faced when cleaning up toxically polluted sites;

F. whereas ageing is the result of an increased life expectancy due to progress in living conditions and in modern medicine, and is one of the greatest political, social, and economic challenges of the 21st century for European societies; whereas by 2025 more than 20 % of Europeans will be 65 or older, with a particularly rapid increase in numbers of people who are in their 80s or older, which will lead to a fundamentally different balance between generations within our societies, and whereas it is in the interest of society that older people remain healthy and active for as long as possible;

G. whereas in the long-term, the current trend leans towards developing smart and autonomous machines, with the capacity to be trained and make decisions independently, holds not only economic advantages but also a variety of concerns regarding their direct and indirect effects on society as a whole;

H. whereas machine learning offers enormous economic and innovative benefits for society by vastly improving the ability to analyse data, while also raising challenges to ensure non-discrimination, due process, transparency and understandability in decision-making processes;

I. whereas similarly, assessments of economic shifts and the impact on employment as a result of robotics and machine learning need to be assessed; whereas, despite the undeniable advantages afforded by robotics, its implementation may entail a transformation of the labour market and a need to reflect on the future of education, employment, and social policies accordingly;

J. whereas the widespread use of robots might not automatically lead to job replacement, but lower skilled jobs in labour-intensive sectors are likely to be more vulnerable to automation; whereas this trend could bring production processes back to the EU; whereas research has demonstrated that employment grows significantly faster in occupations that use computers more; whereas the automation of jobs has the potential to liberate people from manual monotone labour allowing them to shift direction towards more creative and meaningful tasks; whereas automation requires governments to invest in education and other reforms in order to improve reallocation of the types of skills that the workers of tomorrow will need;

K. whereas in the face of increasing divisions in society, with a shrinking middle class, it is important to bear in mind that developing robotics may lead to a high concentration of wealth and influence in the hands of a minority;

L. whereas the development of robotics and AI will definitely influence the landscape of the workplace what may create new liability concerns and eliminate others; whereas the legal responsibility need to be clarified from both business sight model, as well as the workers design pattern, in case emergencies or problems occur;

M. whereas the trend towards automation requires that those involved in the development and commercialisation of AI applications build in security and ethics at the outset, thereby recognizing that they must be prepared to accept legal liability for the quality of the technology they produce;

N. whereas Regulation (EU) 2016/679 of the European Parliament and of the Council[322] (the General Data Protection Regulation) sets out a legal framework to protect personal data; whereas further aspects of data access and the protection of personal data and privacy might still need to be addressed, given that privacy concerns might still arise from applications and appliances communicating with each other and with databases without human intervention;

O. whereas the developments in robotics and AI can and should be designed in such a way that they preserve the dignity, autonomy and self-determination of the individual, especially in the fields of human care and companionship, and in the context of medical appliances, 'repairing' or enhancing human beings;

P. whereas ultimately there is a possibility that in the long-term, AI could surpass human intellectual capacity;

Q. whereas further development and increased use of automated and algorithmic decision-making undoubtedly has an impact on the choices that a private person (such as a business or an internet user) and an administrative, judicial or other public authority take in rendering their final decision of a consumer, business or authoritative nature; whereas safeguards and the possibility of human control and verification need to be built into the process of automated and algorithmic decision-making;

R. whereas several foreign jurisdictions, such as the US, Japan, China and South Korea, are considering, and to a certain extent have already taken, regulatory action with respect to robotics and AI, and whereas some Member States have also started to reflect on possibly drawing up legal standards or carrying out legislative changes in order to take account of emerging applications of such technologies;

S. whereas the European industry could benefit from an efficient, coherent and transparent approach to regulation at Union level, providing predictable and sufficiently clear conditions under which enterprises could develop applications and plan their business models on a European scale while ensuring that the Union and its Member States maintain control over the regulatory standards to be set, so as not to be forced to adopt and live with standards set by others, that is to say the third countries which are also at the forefront of the development of robotics and AI;

General principles

T. whereas Asimov's Laws[323] must be regarded as being directed at the designers, producers and operators of robots, including robots assigned with built-in autonomy and self-learning, since those laws cannot be converted into machine code;

U. whereas a series of rules, governing in particular liability, transparency and accountability, are useful, reflecting the intrinsically European and universal humanistic values that

---

[322] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[323] (1) A robot may not injure a human being or, through inaction, allow a human being to come to harm. (2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law. (3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws (See: I.Asimov, Runaround, 1943) and (0) A robot may not harm humanity, or, by inaction, allow humanity to come to harm.

characterise Europe's contribution to society, are necessary; whereas those rules must not affect the process of research, innovation and development in robotics;

V. whereas the Union could play an essential role in establishing basic ethical principles to be respected in the development, programming and use of robots and AI and in the incorporation of such principles into Union regulations and codes of conduct, with the aim of shaping the technological revolution so that it serves humanity and so that the benefits of advanced robotics and AI are broadly shared, while as far as possible avoiding potential pitfalls;

W. Whereas a Charter on Robotics is annexed to this resolution, drawn up with the assistance of the Scientific Foresight Unit (STOA), European Parliamentary Research Service, which proposes a code of ethical conduct for robotics engineers, a code for research ethics committees, a 'licence' for designers and a 'license' for users;

X. whereas a gradualist, pragmatic and cautious approach of the type advocated by Jean Monnet[324] should be adopted for the Union with regard to future initiatives on robotics and AI so as to ensure that we do not stifle innovation;

Y. whereas it is appropriate, in view of the stage reached in the development of robotics and AI, to start with civil liability issues;

Liability

Z. whereas, thanks to the impressive technological advances of the last decade, not only are today's robots able to perform activities which used to be typically and exclusively human, but the development of certain autonomous and cognitive features – e.g. the ability to learn from experience and take quasi-independent decisions – has made them more and more similar to agents that interact with their environment and are able to alter it significantly; whereas, in such a context, the legal responsibility arising through a robot's harmful action becomes a crucial issue;

AA. whereas a robot's autonomy can be defined as the ability to take decisions and implement them in the outside world, independently of external control or influence; whereas this autonomy is of a purely technological nature and its degree depends on how sophisticated a robot's interaction with its environment has been designed to be;

AB. whereas the more autonomous robots are, the less they can be considered to be simple tools in the hands of other actors (such as the manufacturer, the operator, the owner, the user, etc.); whereas this, in turn, questions whether the ordinary rules on liability are sufficient or whether it calls for new principles and rules to provide clarity on the legal liability of various actors concerning responsibility for the acts and omissions of robots where the cause cannot be traced back to a specific human actor and whether the acts or omissions of robots which have caused harm could have been avoided;

AC. whereas, ultimately, the autonomy of robots raises the question of their nature in the light of the existing legal categories or whether a new category should be created, with its own specific features and implications;

AD. whereas under the current legal framework robots cannot be held liable per se for acts or omissions that cause damage to third parties; whereas the existing rules on liability cover

[324] Cf. the Schuman Declaration (1950): "Europe will not be made all at once, or according to a single plan. It will be built through concrete achievements which first create a de facto solidarity."

cases where the cause of the robot's act or omission can be traced back to a specific human agent such as the manufacturer, the operator, the owner or the user and where that agent could have foreseen and avoided the robot's harmful behaviour; whereas, in addition, manufacturers, operators, owners or users could be held strictly liable for acts or omissions of a robot;

AE. whereas according to the current legal framework for product liability - where the producer of a product is liable for a malfunction- and rules governing liability for harmful actions - where the user of a product is liable for a behaviour that leads to harm- apply to damages caused by robots or AI;

AF. whereas in the scenario where a robot can take autonomous decisions, the traditional rules will not suffice to give rise to legal liability for damage caused by a robot, since they would not make it possible to identify the party responsible for providing compensation and to require that party to make good the damage it has caused;

AG. whereas the shortcomings of the current legal framework are also apparent in the area of contractual liability insofar as machines designed to choose their counterparts, negotiate contractual terms, conclude contracts and decide whether and how to implement them, make the traditional rules inapplicable; whereas this highlights the need for new, efficient and up-to-date ones, which should comply with technological developments and innovations that have recently arisen and are used on the market;

AH. whereas, as regards non-contractual liability, Directive 85/374/EEC can cover only damage caused by a robot's manufacturing defects and on condition that the injured person is able to prove the actual damage, the defect in the product and the causal relationship between damage and defect, therefore strict liability or liability without fault framework may not be sufficient;

AI. whereas, notwithstanding the scope of Directive 85/374/EEC, the current legal framework would not be sufficient to cover the damage caused by the new generation of robots, insofar as they can be equipped with adaptive and learning abilities entailing a certain degree of unpredictability in their behaviour, since those robots would autonomously learn from their own variable experience and interact with their environment in a unique and unforeseeable manner;

General principles concerning the development of robotics and artificial intelligence for civil use

1. Calls on the Commission to propose common Union definitions of cyber physical systems, autonomous systems, smart autonomous robots and their subcategories by taking into consideration the following characteristics of a smart robot:

   – the acquisition of autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and the trading and analysing of those data;

   – self-learning from experience and by interaction (optional criterion);

   – at least a minor physical support;

   – the adaptation of its behaviour and actions to the environment;

   – absence of life in the biological sense;

2. Considers that a comprehensive Union system of registration of advanced robots should be introduced within the Union's internal market where relevant and necessary for specific categories of robots, and calls on the Commission to establish criteria for the classification of robots that would need to be registered; in this context, calls on the Commission to investigate whether it would be desirable for the registration system and the register to be managed by a designated EU Agency for Robotics and Artificial Intelligence;

3. Stresses that the development of robot technology should focus on complementing human capabilities and not on replacing them; considers it essential, in the development of robotics and AI, to guarantee that humans have control over intelligent machines at all times; considers that special attention should be paid to the possible development of an emotional connection between humans and robots – particularly in vulnerable groups (children, the elderly and people with disabilities) – and highlights the issues raised by the serious emotional or physical impact that this emotional attachment could have on humans;

4. Emphasises that a Union-level approach can facilitate development by avoiding fragmentation in the internal market and at the same time underlines the importance of the principle of mutual recognition in the cross-border use of robots and robotic systems; recalls that testing, certification and market approval should only be required in a single Member State; stresses that this approach should be accompanied by effective market surveillance;

5. Stresses the importance of measures to help small and medium-sized enterprises and start-ups in the robotics sector that create new market segments in this sector or make use of robots;

Research and innovation

6. Underlines that many robotic applications are still in an experimental phase; welcomes the fact that more and more research projects are being funded by the Member States and the Union; considers it to be essential that the Union, together with the Member States by virtue of public funding, remains a leader in research in robotics and AI; calls on the Commission and the Member States to strengthen financial instruments for research projects in robotics and ICT, including public-private partnerships, and to implement in their research policies the principles of open science and responsible ethical innovation; emphasises that sufficient resources need to be devoted to the search for solutions to the social, ethical, legal and economic challenges that the technological development and its applications raise;

7. Calls on the Commission and the Member States to foster research programmes, to stimulate research into the possible long-term risks and opportunities of robotics and AI technologies and to encourage the initiation of a structured public dialogue on the consequences of developing those technologies as soon as possible; calls on the Commission to increase its support in the mid-term review of the Multiannual Financial Framework for the Horizon 2020 funded SPARC programme; calls on the Commission and the Member States to combine their efforts in order to carefully monitor and guarantee a smoother transition for these technologies from research to commercialisation and use on the market after appropriate safety evaluations in compliance with the precautionary principle;

8. Stresses that innovation in robotics and AI and the integration of robotics and AI technology within the economy and the society require digital infrastructure that provides ubiquitous connectivity; calls on the Commission to set a framework that will meet the connectivity requirements for the Union's digital future and to ensure that access to broadband and 5G networks is fully in line with the net neutrality principle;

9. Strongly believes that interoperability between systems, devices and cloud services, based on security and privacy by design is essential for real time data flows enabling robots and AI to become more flexible and autonomous; asks the Commission to promote an open environment, from open standards and innovative licensing models, to open platforms and transparency, in order to avoid lock-in in proprietary systems that restrain interoperability;

Ethical principles

10. Notes that the potential for empowerment through the use of robotics is nuanced by a set of tensions or risks and should be seriously assessed from the point of view of human safety, health and security; freedom, privacy, integrity and dignity; self-determination and non-discrimination, and personal data protection;

11. Considers that the existing Union legal framework should be updated and complemented, where appropriate, by guiding ethical principles in line with the complexity of robotics and its many social, medical and bioethical implications; is of the view that a clear, strict and efficient guiding ethical framework for the development, design, production, use and modification of robots is needed to complement the legal recommendations of the report and the existing national and Union *acquis*; proposes, in the annex to the resolution, a framework in the form of a charter consisting of a code of conduct for robotics engineers, of a code for research ethics committees when reviewing robotics protocols and of model licences for designers and users;

12. Highlights the principle of transparency, namely that it should always be possible to supply the rationale behind any decision taken with the aid of AI that can have a substantive impact on one or more persons' lives; considers that it must always be possible to reduce the AI system´s computations to a form comprehensible by humans; considers that advanced robots should be equipped with a 'black box' which records data on every transaction carried out by the machine, including the logic that contributed to its decisions;

13. Points out that the guiding ethical framework should be based on the principles of beneficence, non-maleficence, autonomy and justice, on the principles and values enshrined in Article 2 of the Treaty on European Union and in the Charter of Fundamental Rights, such as human dignity, equality, justice and equity, non-discrimination, informed consent, private and family life and data protection, as well as on other underlying principles and values of the Union law, such as non-stigmatisation, transparency, autonomy, individual responsibility and social responsibility, and on existing ethical practices and codes;

14. Considers that special attention should be paid to robots that represent a significant threat to confidentiality owing to their placement in traditionally protected and private spheres and because they are able to extract and send personal and sensitive data;

A European Agency

15. Believes that enhanced cooperation between the Member States and the Commission is necessary in order to guarantee coherent cross-border rules in the Union which encourage the collaboration between European industries and allow the deployment in the whole Union of robots which are consistent with the required levels of safety and security, as well as the ethical principles enshrined in Union law;

16. Asks the Commission to consider the designation of a European Agency for Robotics and Artificial Intelligence in order to provide the technical, ethical and regulatory expertise needed to support the relevant public actors, at both Union and Member State level, in their efforts to ensure a timely, ethical and well-informed response to the new opportunities and

challenges, in particular those of a cross-border nature, arising from technological developments in robotics, such as in the transport sector;

17. Considers that the potential of and the problems linked to robotics use and the present investment dynamics justify providing the European Agency with a proper budget and staffing it with regulators and external technical and ethical experts dedicated to the cross-sectorial and multidisciplinary monitoring of robotics-based applications, identifying standards for best practice, and, where appropriate, recommending regulatory measures, defining new principles and addressing potential consumer protection issues and systematic challenges; asks the Commission (and the European Agency, if created) to report to the European Parliament on the latest developments in robotics and on any actions that need to be taken on an annual basis;

Intellectual property rights and the flow of data

18. Notes that there are no legal provisions that specifically apply to robotics, but that existing legal regimes and doctrines can be readily applied to robotics, although some aspects appear to call for specific consideration; calls on the Commission to support a horizontal and technologically neutral approach to intellectual property applicable to the various sectors in which robotics could be employed;

19. Calls on the Commission and the Member States to ensure that civil law regulations in the robotics sector are consistent with the General Data Protection Regulation and in line with the principles of necessity and proportionality; calls on the Commission and the Member States to take into account the rapid technological evolution in the field of robotics, including the advancement of cyber-physical systems, and to ensure that Union law does not stay behind the curve of technological development and deployment;

20. Emphasises that the right to respect for private life and to the protection of personal data as enshrined in Article 7 and 8 of the Charter and in Article 16 of the Treaty on the Functioning of the European Union (TFEU) apply to all areas of robotics and that the Union legal framework for data protection must be fully complied with; asks in this regard for clarification within the implementation framework of the GDPR of rules and criteria regarding the use of cameras and sensors in robots; calls on the Commission to make sure that the data protection principles such as privacy by design and privacy by default, data minimisation, purpose limitation, as well as transparent control mechanisms for data subjects and appropriate remedies in compliance with Union data protection law and are followed and appropriate recommendations and standards are fostered and are integrated into Union policies;

21. Stresses that the free movement of data is paramount to the digital economy and development in the robotics and AI sector; stresses that a high level of security in robotics systems, including their internal data systems and data flows, is crucial to the appropriate use of robots and AI; emphasises that the protection of networks of interconnected robots and AI has to be ensured to prevent potential security breaches; emphasises that a high level of security and protection of personal data together with due regard for privacy in communication between humans, robots and AI are fundamental; stresses the responsibility of designers of robotics and AI to develop products to be safe, secure and fit for purpose; calls on the Commission and the Member States to support and incentivise the development of the necessary technology, including security by design;

Standardisation, safety and security

22. Highlights that the issue of setting standards and granting interoperability is key for future competition in the field of AI and robotics technologies; calls on the Commission to continue

to work on the international harmonisation of technical standards, in particular together with the European Standardisation Organisations and the International Standardisation Organisation, in order to foster innovation, to avoid fragmentation of the internal market and to guarantee a high level of product safety and consumer protection including where appropriate minimum safety standards in the work environment; stresses the importance of lawful reverse-engineering and open standards, in order to maximise the value of innovation and to ensure that robots can communicate with each other; welcomes, in this respect, the setting up of special technical committees, such as ISO/TC 299 Robotics, dedicated exclusively to developing standards on robotics;

23. Emphasises that testing robots in real-life scenarios is essential for the identification and assessment of the risks they might entail, as well as of their technological development beyond a pure experimental laboratory phase; underlines, in this regard, that testing of robots in real-life scenarios, in particular in cities and on roads, raises a large number of issues, including barriers that slow down the development of those testing phases and requires an effective strategy and monitoring mechanism; calls on the Commission to draw up uniform criteria across all Member States which individual Member States should use in order to identify areas where experiments with robots are permitted, in compliance with the precautionary principle;

Autonomous means of transport

a) Autonomous vehicles

24. Underlines that autonomous transport covers all forms of remotely piloted, automated, connected and autonomous ways of road, rail, waterborne and air transport, including vehicles, trains, vessels, ferries, aircrafts, drones, as well as all future forms of developments and innovations in this sector;

25. Considers that the automotive sector is in most urgent need of efficient Union and global rules to ensure the cross-border development of automated and autonomous vehicles so as to fully exploit their economic potential and benefit from the positive effects of technological trends; emphasises that fragmented regulatory approaches would hinder implementation of autonomous transport systems and jeopardise European competitiveness;

26. Draws attention to the fact that driver reaction time in the event of an unplanned takeover of control of the vehicle is of vital importance and calls, therefore, on the stakeholders to provide for realistic values determining safety and liability issues;

27. Takes the view that the switch to autonomous vehicles will have an impact on the following aspects: civil responsibility (liability and insurance), road safety, all topics related to environment (e.g. energy efficiency, use of renewable technologies and energy sources), issues related to data (e.g. access to data, protection of data, privacy and sharing of data), issues related to ICT infrastructure (e.g. high density of efficient and reliable communication) and employment (e.g. creation and losses of jobs, training of heavy goods vehicles drivers for the use of automated vehicles); emphasises that substantial investments in roads, energy and ICT infrastructure will be required; calls on the Commission to consider the above-mentioned aspects in its work on autonomous vehicles;

28. Underlines the critical importance of reliable positioning and timing information provided by the European satellite navigation programmes Galileo and EGNOS for the implementation of autonomous vehicles, urges, in this regard, the finalisation and launch of the satellites which are needed in order to complete the European Galileo positioning system;

29. Draws attention to the high added value provided by autonomous vehicles for persons with reduced mobility, as such vehicles allow them to participate more effectively in individual road transport and thereby facilitate their daily lives;

b) Drones (RPAS)

30. Acknowledges the positive advances in drone technology, particularly in the field of search and rescue; stresses the importance of a Union framework for drones to protect the safety, security and privacy of the citizens of the Union, and calls on the Commission to follow-up on the recommendations of Parliament's resolution of 29 October 2015 on safe use of remotely piloted aircraft systems (RPAS), commonly known as unmanned aerial vehicles (UAVs), in the field of civil aviation[325]; urges the Commission to provide assessments of the safety issues connected with the widespread use of drones; calls on the Commission to examine the need to introduce an obligatory tracking and identification system for RPAS which enables aircraft's real-time positions during use to be determined; recalls, that the homogeneity and safety of unmanned aircrafts should be ensured by the measures set out in Regulation (EC) No 216/2008 of the European Parliament and of the Council[326];

Care robots

31. Underlines that elder care robot research and development has, in time, become more mainstream and cheaper, producing products with greater functionality and broader consumer acceptance; notes the wide range of applications of such technologies providing prevention, assistance, monitoring, stimulation, and companionship to elderly people and people with disabilities as well as to people suffering from dementia, cognitive disorders, or memory loss;

32. Points out that human contact is one of the fundamental aspects of human care; believes that replacing the human factor with robots could dehumanise caring practices, on the other hand, recognises that robots could perform automated care tasks and could facilitate the work of care assistants, while augmenting human care and making the rehabilitation process more targeted, thereby enabling medical staff and caregivers to devote more time to diagnosis and better planned treatment options; stresses that despite the potential of robotics to enhance the mobility and integration of people with disabilities and elderly people, humans will still be needed in caregiving and will continue to provide an important source of social interaction that is not fully replaceable;

Medical robots

33. Underlines the importance of appropriate education, training and preparation for health professionals, such as doctors and care assistants, in order to secure the highest degree of professional competence possible, as well as to safeguard and protect patients' health; underlines the need to define the minimum professional requirements that a surgeon must meet in order to operate and be allowed to use surgical robots; considers it vital to respect the principle of the supervised autonomy of robots, whereby the initial planning of treatment and the final decision regarding its execution will always remain with a human

[325] Texts adopted, P8_TA(2015)0390.
[326] Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (OJ L 79, 19.3.2008, p. 1).

surgeon; emphasises the special importance of training for users to allow them to familiarise themselves with the technological requirements in this field; draws attention to the growing trend towards self-diagnosis using a mobile robot and, consequently, to the need for doctors to be trained in dealing with self-diagnosed cases; considers that the use of such technologies should not diminish or harm the doctor-patient relationship, but should provide doctors with assistance in diagnosing and/or treating patients with the aim of reducing the risk of human error and of increasing the quality of life and life expectancy;

34. Believes that medical robots continue to make inroads into the provision of high accuracy surgery and in performing repetitive procedures and that they have the potential to improve outcomes in rehabilitation, and provide highly effective logistical support within hospitals; notes that medical robots have the potential also to reduce healthcare costs by enabling medical professionals to shift their focus from treatment to prevention and by making more budgetary resources available for better adjustment to the diversity of patients' needs, continuous training of the healthcare professionals and research;

35. Calls on the Commission to ensure that the procedures for testing new medical robotic devices are safe, particularly in the case of devices that are implanted in the human body, before the date on which Regulation (EU) 2017/745 on medical devices becomes applicable;

Human repair and enhancement

36. Notes the great advances delivered by and further potential of robotics in the field of repairing and compensating for damaged organs and human functions, but also the complex questions raised in particular by the possibilities of human enhancement, as medical robots and particularly cyber physical systems (CPS) may change our concepts about the healthy human body since they can be worn directly on or implanted in the human body; underlines the importance of urgently establishing in hospitals and in other health care institutions appropriately staffed committees on robot ethics tasked with considering and assisting in resolving unusual, complicated ethical problems involving issues that affect the care and treatment of patients; calls on the Commission and the Member States to develop guidelines to aid in the establishment and functioning of such committees;

37. Points out that for the field of vital medical applications such as robotic prostheses, continuous, sustainable access to maintenance, enhancement and, in particular, software updates that fix malfunctions and vulnerabilities needs to be ensured;

38. Recommends the creation of independent trusted entities to retain the means necessary to provide services to persons carrying vital and advanced medical appliances, such as maintenance, repairs and enhancements, including software updates, especially in the case where such services are no longer carried out by the original supplier; suggests creating an obligation for manufacturers to supply these independent trusted entities with comprehensive design instructions including source code, similar to the legal deposit of publications to a national library;

39. Draws attention to the risks associated with the possibility that CPS integrated into the human body may be hacked or switched off or have their memories wiped, because this could endanger human health, and in extreme cases even human life, and stresses therefore the priority that must be attached to protecting such systems;

40. Underlines the importance of guaranteeing equal access for all people to such technological innovations, tools and interventions; calls on the Commission and the Member States to promote the development of assistive technologies in order to facilitate the development

and adoption of these technologies by those who need them, in accordance with Article 4 of the UN Convention on the Rights of Persons with Disabilities, to which the Union is party;

Education and employment

41. Draws attention to the Commission's forecast that by 2020 Europe might be facing a shortage of up to 825 000 ICT professionals and that 90 % of jobs will require at least basic digital skills; welcomes the Commission's initiative of proposing a roadmap for the possible use and revision of a Digital Competence framework and descriptors of Digital Competences for all levels of learners, and calls upon the Commission to provide significant support for the development of digital abilities in all age groups and irrespective of employment status, as a first step towards better aligning labour market shortages and demand; stresses that the growth in the robotics requires Member States to develop more flexible training and education systems so as to ensure that skill strategies match the needs of the robot economy;

42. Considers that getting more young women interested in a digital career and placing more women in digital jobs would benefit the digital industry, women themselves and Europe's economy; calls on the Commission and the Member States to launch initiatives in order to support women in ICT and to boost their e-skills;

43. Calls on the Commission to start analysing and monitoring medium- and long-term job trends more closely, with a special focus on the creation, displacement and loss of jobs in the different fields/areas of qualification in order to know in which fields jobs are being created and those in which jobs are being lost as a result of the increased use of robots;

44. Highlights the importance of foreseeing changes to society, bearing in mind the effect that the development and deployment of robotics and AI might have; asks the Commission to analyse different possible scenarios and their consequences on the viability of the social security systems of the Member States;

45. Emphasises the importance of the flexibility of skills and of social, creative and digital skills in education; is certain that, in addition to schools imparting academic knowledge, lifelong learning needs to be achieved through lifelong activity;

46. Notes the great potential of robotics for the improvement of safety at work by transferring a number of hazardous and harmful tasks from humans to robots, but at the same time, notes their potential for creating a set of new risks owing to the increasing number of human-robot interactions at the workplace; underlines in this regard the importance of applying strict and forward-looking rules for human-robot interactions in order to guarantee health, safety and the respect of fundamental rights at the workplace;

Environmental impact

47. Notes that the development of robotics and AI should be done in such a manner that the environmental impact is limited through effective energy consumption, energy efficiency by promoting the use of renewable energy and of scarce materials, and minimal waste, such as electric and electronic waste, and reparability; therefore encourages the Commission to incorporate the principles of a circular economy into any Union policy on robotics; notes that the use of robotics will also have a positive impact on the environment, especially in the fields of agriculture, food supply and transport, notably through the reduced size of machinery and the reduced use of fertilizers, energy and water, as well as through precision farming and route optimisation;

48. Stresses that CPS will lead to the creation of energy and infrastructure systems that are able to control the flow of electricity from producer to consumer, and will also result in the creation of energy 'prosumers', who both produce and consume energy; thus allowing for major environmental benefits;

Liability

49. Considers that the civil liability for damage caused by robots is a crucial issue which also needs to be analysed and addressed at Union level in order to ensure the same degree of efficiency, transparency and consistency in the implementation of legal certainty throughout the European Union for the benefit of citizens, consumers and businesses alike;

50. Notes that development of robotics technology will require more understanding for the common ground needed around joint human-robot activity, which should be based on two core interdependent relationships, namely predictability and directability; points out that these two interdependent relationships are crucial for determining what information need to be shared between humans and robots and how a common basis between humans and robots can be achieved in order to enable smooth human-robot joint action;

51. Asks the Commission to submit, on the basis of Article 114 TFEU, a proposal for a legislative instrument on legal questions related to the development and use of robotics and AI foreseeable in the next 10 to 15 years, combined with non-legislative instruments such as guidelines and codes of conduct as referred to in recommendations set out in the Annex;

52. Considers that, whatever legal solution it applies to the civil liability for damage caused by robots in cases other than those of damage to property, the future legislative instrument should in no way restrict the type or the extent of the damages which may be recovered, nor should it limit the forms of compensation which may be offered to the aggrieved party, on the sole grounds that damage is caused by a non-human agent;

53. Considers that the future legislative instrument should be based on an in-depth evaluation by the Commission determining whether the strict liability or the risk management approach should be applied;

54. Notes at the same time that strict liability requires only proof that damage has occurred and the establishment of a causal link between the harmful functioning of the robot and the damage suffered by the injured party;

55. Notes that the risk management approach does not focus on the person "who acted negligently" as individually liable but on the person who is able, under certain circumstances, to minimise risks and deal with negative impacts;

56. Considers that, in principle, once the parties bearing the ultimate responsibility have been identified, their liability should be proportional to the actual level of instructions given to the robot and of its degree of autonomy, so that the greater a robot's learning capability or autonomy, and the longer a robot's training, the greater the responsibility of its trainer should be; notes, in particular, that skills resulting from "training" given to a robot should be not confused with skills depending strictly on its self-learning abilities when seeking to identify the person to whom the robot's harmful behaviour is actually attributable; notes that at least at the present stage the responsibility must lie with a human and not a robot;

57. Points out that a possible solution to the complexity of allocating responsibility for damage caused by increasingly autonomous robots could be an obligatory insurance scheme, as is already the case, for instance, with cars; notes, nevertheless, that unlike the insurance

system for road traffic, where the insurance covers human acts and failures, an insurance system for robotics should take into account all potential responsibilities in the chain;

58. Considers that, as is the case with the insurance of motor vehicles, such an insurance system could be supplemented by a fund in order to ensure that reparation can be made for damage in cases where no insurance cover exists; calls on the insurance industry to develop new products and types of offers that are in line with the advances in robotics;

59. Calls on the Commission, when carrying out an impact assessment of its future legislative instrument, to explore, analyse and consider the implications of all possible legal solutions, such as:

a) establishing a compulsory insurance scheme where relevant and necessary for specific categories of robots whereby, similarly to what already happens with cars, producers, or owners of robots would be required to take out insurance cover for the damage potentially caused by their robots;

b) ensuring that a compensation fund would not only serve the purpose of guaranteeing compensation if the damage caused by a robot was not covered by insurance;

c) allowing the manufacturer, the programmer, the owner or the user to benefit from limited liability if they contribute to a compensation fund, as well as if they jointly take out insurance to guarantee compensation where damage is caused by a robot;

d) deciding whether to create a general fund for all smart autonomous robots or to create an individual fund for each and every robot category, and whether a contribution should be paid as a one-off fee when placing the robot on the market or whether periodic contributions should be paid during the lifetime of the robot;

e) ensuring that the link between a robot and its fund would be made visible by an individual registration number appearing in a specific Union register, which would allow anyone interacting with the robot to be informed about the nature of the fund, the limits of its liability in case of damage to property, the names and the functions of the contributors and all other relevant details;

f) creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently;

International aspects

60. Notes that current general private international law rules on traffic accidents applicable within the Union do not urgently need substantive modification to accommodate the development of autonomous vehicles, however, simplifying the current dual system for defining applicable law (based on Regulation (EC) No 864/2007 of the European Parliament and of the Council[327] and the Hague Convention of 4 May 1971 on the law applicable to traffic accidents) would improve legal certainty and limit possibilities for forum shopping;

61. Notes the need to consider amendments to international agreements such as the Vienna

[327] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (OJ L 199, 31.7.2007, p. 40).

Convention on Road Traffic of 8 November 1968 and the Hague Convention on the law applicable to traffic accidents;

62. Expects the Commission to ensure that Member States implement international law, such as the Vienna Convention on Road Traffic, which needs to be amended, in a uniform manner in order to make driverless driving possible, and calls on the Commission, the Member States and the industry to implement the objectives of the Amsterdam Declaration as soon as possible;

63. Strongly encourages international cooperation in the scrutiny of societal, ethical and legal challenges and thereafter setting regulatory standards under the auspices of the United Nations;

64. Points out that the restrictions and conditions laid down in Regulation (EC) No 428/2009 of the European Parliament and of the Council[328] on the trade in dual-use items – goods, software and technology that can be used for both civilian and military applications and/or can contribute to the proliferation of weapons of mass destruction – should apply to applications of robotics as well;

Final aspects

65. Requests, on the basis of Article 225 TFEU, the Commission to submit, on the basis of Article 114 TFEU, a proposal for a directive on civil law rules on robotics, following the recommendations set out in the Annex hereto;

66. Confirms that the recommendations respect fundamental rights and the principle of subsidiarity;

67. Considers that the requested proposal would have financial implications if a new European agency is set up;

68. Instructs its President to forward this resolution and the accompanying recommendations to the Commission and the Council.

[328] Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (OJ L 134, 29.5.2009, p. 1).

ANNEX TO THE RESOLUTION:
RECOMMENDATIONS AS TO THE CONTENT OF THE PROPOSAL REQUESTED

Definition and classification of 'smart robots'

A common European definition for smart autonomous robots should be established, where appropriate including definitions of its subcategories, taking into consideration the following characteristics:

- the capacity to acquire autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and the analysis of those data;
- the capacity to learn through experience and interaction;
- the form of the robot's physical support;
- the capacity to adapt its be2017/2394 and Directive 2009/22/EC haviour and actions to the environment.

Registration of smart robots

For the purposes of traceability and in order to facilitate the implementation of further recommendations, a system of registration of advanced robots should be introduced, based on the criteria established for the classification of robots. The system of registration and the register should be Union-wide, covering the internal market, and could be managed by a designated EU Agency for Robotics and Artificial Intelligence in case such an Agency is created.

Civil law liability

Any chosen legal solution applied to the liability of robots and of artificial intelligence in cases other than those of damage to property should in no way restrict the type or the extent of the damages which may be recovered, nor should it limit the forms of compensation which may be offered to the aggrieved party on the sole grounds that damage is caused by a non-human agent.

The future legislative instrument should be based on an in-depth evaluation by the Commission defining whether the strict liability or the risk management approach should be applied.

An obligatory insurance scheme, which could be based on the obligation of the producer to take out insurance for the autonomous robots it produces, should be established.

The insurance system should be supplemented by a fund in order to ensure that damages can be compensated for in cases where no insurance cover exists.

Any policy decision on the civil liability rules applicable to robots and artificial intelligence should be taken with due consultation of a European-wide research and development project dedicated to robotics and neuroscience, with scientists and experts able to assess all related risks and consequences;

Interoperability, access to code and intellectual property rights

The interoperability of network-connected autonomous robots that interact with each other should be ensured. Access to the source code, input data, and construction details should be available when needed**,** to investigate accidents and damage caused by smart robots, as well as in order to ensure their continued operation, availability, reliability, safety and security.

Charter on Robotics

The Commission, when proposing legal acts relating to robotics, should take into account the principles enshrined in the following Charter on Robotics.

CHARTER ON ROBOTICS

The proposed code of ethical conduct in the field of robotics will lay the groundwork for the identification, oversight and compliance with fundamental ethical principles from the design and development phase.

The framework, drafted in consultation with a European-wide research and development project dedicated to robotics and neuroscience, must be designed in a reflective manner that allows individual adjustments to be made on a case-by-case basis in order to assess whether a given behaviour is right or wrong in a given situation and to take decisions in accordance with a pre-set hierarchy of values.

The code should not replace the need to tackle all major legal challenges in this field, but should have a complementary function. It will, rather, facilitate the ethical categorisation of robotics, strengthen the responsible innovation efforts in this field and address public concerns.

Special emphasis should be placed on the research and development phases of the relevant technological trajectory (design process, ethics review, audit controls, etc.). It should aim to address the need for compliance by researchers, practitioners, users and designers with ethical standards, but also introduce a procedure for devising a way to resolve the relevant ethical dilemmas and to allow these systems to function in an ethically responsible manner.

CODE OF ETHICAL CONDUCT FOR ROBOTICS ENGINEERS

PREAMBLE

The Code of Conduct invites all researchers and designers to act responsibly and with absolute consideration for the need to respect the dignity, privacy and safety of humans.

The Code asks for close cooperation among all disciplines in order to ensure that robotics research is undertaken in the European Union in a safe, ethical and effective manner.

The Code of Conduct covers all research and development activities in the field of robotics.

The Code of Conduct is voluntary and offers a set of general principles and guidelines for actions to be taken by all stakeholders.

Robotics research funding bodies, research organisations, researchers and ethics committees are encouraged to consider, at the earliest stages, the future implications of the technologies or objects being researched and to develop a culture of responsibility with a view to the challenges and opportunities that may arise in the future.

Public and private robotics research funding bodies should request that a risk assessment be performed and presented along with each submission of a proposal for funding for robotics research. Such a code should consider humans, not robots, as the responsible agents.

Researchers in the field of robotics should commit themselves to the highest ethical and professional conduct and abide by the following principles:

Beneficence – robots should act in the best interests of humans;

Non-maleficence – the doctrine of 'first, do no harm', whereby robots should not harm a human;

Autonomy – the capacity to make an informed, un-coerced decision about the terms of interaction with robots;

Justice – fair distribution of the benefits associated with robotics and affordability of homecare and healthcare robots in particular.

Fundamental Rights

Robotics research activities should respect fundamental rights and be conducted in the interests of the well-being and self-determination of the individual and society at large in their design, implementation, dissemination and use. Human dignity and autonomy – both physical and psychological – is always to be respected.

Precaution

Robotics research activities should be conducted in accordance with the precautionary principle, anticipating potential safety impacts of outcomes and taking due precautions, proportional to the level of protection, while encouraging progress for the benefit of society and the environment.

Inclusiveness

Robotics engineers guarantee transparency and respect for the legitimate right of access to information by all stakeholders. Inclusiveness allows for participation in decision-making processes by all stakeholders involved in or concerned by robotics research activities.

Accountability

Robotics engineers should remain accountable for the social, environmental and human health impacts that robotics may impose on present and future generations.

Safety

Robot designers should consider and respect people's physical wellbeing, safety, health and rights. A robotics engineer must preserve human wellbeing, while also respecting human rights, and disclose promptly factors that might endanger the public or the environment.

Reversibility

Reversibility, being a necessary condition of controllability, is a fundamental concept when programming robots to behave safely and reliably. A reversibility model tells the robot which actions are reversible and how to reverse them if they are. The ability to undo the last action or a sequence of actions allows users to undo undesired actions and get back to the 'good' stage of their work.

Privacy

The right to privacy must always be respected. A robotics engineer should ensure that private information is kept secure and only used appropriately. Moreover, a robotics engineer should guarantee that individuals are not personally identifiable, aside from exceptional circumstances and then only with clear, unambiguous informed consent. Human informed consent should be pursued and obtained prior to any man-machine interaction. As such, robotics designers have a responsibility to develop and follow procedures for valid consent, confidentiality, anonymity, fair treatment and due process. Designers will comply with any requests that any related data be

destroyed, and removed from any datasets.

Maximising benefit and minimising harm

Researchers should seek to maximise the benefits of their work at all stages, from inception through to dissemination. Harm to research participants, human subject, an experiment, trial, or study participant or subject must be avoided. Where risks arise as an unavoidable and integral element of the research, robust risk assessment and management protocols should be developed and complied with. Normally, the risk of harm should be no greater than that encountered in ordinary life, i.e. people should not be exposed to risks greater than or additional to those to which they are exposed in their normal lifestyles. The operation of a robotics system should always be based on a thorough risk assessment process, which should be informed by the precautionary and proportionality principles.

CODE FOR RESEARCH ETHICS COMMITTEES (REC

Principles

Independence

The ethics review process should be independent of the research itself. This principle highlights the need to avoid conflicts of interest between researchers and those reviewing the ethics protocol, and between reviewers and organisational governance structures.

Competence

The ethics review process should be conducted by reviewers with appropriate expertise, taking into account the need for careful consideration of the range of membership and ethics-specific training of RECs.

Transparency and accountability

The review process should be accountable and open to scrutiny. RECs need to recognise their responsibilities and to be appropriately located within organisational structures that give transparency to the REC operation and procedures to maintain and review standards.

The role of a Research Ethics Committee

A REC is normally responsible for reviewing all research involving human participants conducted by individuals employed within or by the institution concerned; ensuring that ethics review is independent, competent and timely; protecting the dignity, rights and welfare of research participants; considering the safety of the researcher(s); considering the legitimate interests of other stakeholders; making informed judgements of the scientific merit of proposals; and making informed recommendations to the researcher if the proposal is found to be wanting in some respect.

The constitution of a Research Ethics Committee

A REC should normally be multidisciplinary; include both men and women; be comprised of members with a broad experience of and expertise in the area of robotics research. The appointment mechanism should ensure that the committee members provide an appropriate balance of scientific expertise, philosophical, legal or ethical backgrounds, and lay views, and that they include at least one member with specialist knowledge in ethics, users of specialist health, education or social services where these are the focus of research activities, and individuals with specific methodological expertise relevant to the research they review; and they must be so constituted that conflicts of interest are avoided.

Monitoring

All research organisations should establish appropriate procedures to monitor the conduct of research which has received ethics approval until it is completed, and to ensure continuing review where the research design anticipates possible changes over time that might need to be addressed. Monitoring should be proportionate to the nature and degree of risk associated with the research. Where a REC considers that a monitoring report raises significant concerns about the ethical conduct of the study, it should request a full and detailed account of the research for full ethics review. Where it is judged that a study is being conducted unethically, the withdrawal of its approval should be considered and its research should be suspended or discontinued.

LICENCE FOR DESIGNERS

- You should take into account the European values of dignity, autonomy and self-determination, freedom and justice before, during and after the process of design, development and delivery of such technologies including the need not to harm, injure, deceive or exploit (vulnerable) users.

- You should introduce trustworthy system design principles across all aspects of a robot's operation, for both hardware and software design, and for any data processing on or off the platform for security purposes.

- You should introduce privacy by design features so as to ensure that private information is kept secure and only used appropriately.

- You should integrate obvious opt-out mechanisms (kill switches) that should be consistent with reasonable design objectives.

- You should ensure that a robot operates in a way that is in accordance with local, national and international ethical and legal principles.

- You should ensure that the robot's decision-making steps are amenable to reconstruction and traceability.

- You should ensure that maximal transparency is required in the programming of robotic systems, as well as predictability of robotic behaviour.

- You should analyse the predictability of a human-robot system by considering uncertainty in interpretation and action and possible robotic or human failures.

- You should develop tracing tools at the robot's design stage. These tools will facilitate accounting and explanation of robotic behaviour, even if limited, at the various levels intended for experts, operators and users.

- You should draw up design and evaluation protocols and join with potential users and stakeholders when evaluating the benefits and risks of robotics, including cognitive, psychological and environmental ones.

- You should ensure that robots are identifiable as robots when interacting with humans.

- You should safeguard the safety and health of those interacting and coming in touch with robotics, given that robots as products should be designed using processes which ensure their safety and security. A robotics engineer must preserve human wellbeing while also

respecting human rights and may not deploy a robot without safeguarding the safety, efficacy and reversibility of the operation of the system.

- You should obtain a positive opinion from a Research Ethics Committee before testing a robot in a real environment or involving humans in its design and development procedures.

LICENCE FOR USERS

- You are permitted to make use of a robot without risk or fear of physical or psychological harm.
- You should have the right to expect a robot to perform any task for which it has been explicitly designed.
- You should be aware that any robot may have perceptual, cognitive and actuation limitations.
- You should respect human frailty, both physical and psychological, and the emotional needs of humans.
- You should take the privacy rights of individuals into consideration, including the deactivation of video monitors during intimate procedures.
- You are not permitted to collect, use or disclose personal information without the explicit consent of the data subject.
- You are not permitted to use a robot in any way that contravenes ethical or legal principles and standards.
- You are not permitted to modify any robot to enable it to function as a weapon.

Directive on digital content and digital services

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) The growth potential of e-commerce in the Union has not yet been fully exploited. The Digital Single Market Strategy for Europe tackles in a holistic manner the major obstacles to the development of cross-border e-commerce in the Union in order to unleash this potential. Ensuring better access for consumers to digital content and digital services, and making it easier for businesses to supply digital content and digital services, can contribute to boosting the Union's digital economy and stimulating overall growth.

(2) Article 26(1) and (2) of the Treaty on the Functioning of the European Union (TFEU) provide that the Union is to adopt measures with the aim of establishing or ensuring the functioning of the internal market, which is to comprise an area without internal frontiers in which the free movement of goods and services is ensured. Article 169(1), and point (a) of Article 169(2), TFEU provide that the Union is to contribute to the attainment of a high level of consumer protection through measures adopted pursuant to Article 114 TFEU in the context of the completion of the internal market. This Directive aims to strike the right balance between achieving a high level of consumer protection and promoting the competitiveness of enterprises, while ensuring respect for the principle of subsidiarity.

(3) Certain aspects concerning contracts for the supply of digital content or digital services should be harmonised, taking as a base a high level of consumer protection, in order to achieve a genuine digital single market, increase legal certainty and reduce transaction costs, in particular for small and medium-sized enterprises ('SMEs').

(4) Businesses, especially SMEs, often face additional costs, stemming from differences in national mandatory consumer contract law rules, and legal uncertainty when offering cross-border digital content or digital services. Businesses also face costs when adapting their contracts to specific mandatory rules for the supply of digital content or digital services, which are already being applied in several Member States, creating differences in scope and content between specific national rules governing such contracts.

(5) Consumers are not always confident when buying cross border and especially when it is done online. One of the major factors for consumers' lack of confidence is uncertainty about their key contractual rights and the lack of a clear contractual framework for digital content or digital services. Many consumers experience problems related to the quality of, or access to, digital content or digital services. For instance, they receive wrong or faulty digital content or digital services, or they are not able to access the digital content or digital service in question. As a result, consumers suffer financial and non-financial detriment.

(6) In order to remedy such problems, both businesses and consumers should be able to rely on fully harmonised contractual rights in certain core areas concerning the supply of digital

content or digital services across the Union. Full harmonisation of some key regulatory aspects would considerably increase legal certainty for consumers and businesses.

(7) Harmonised consumer contract law rules in all Member States would make it easier for businesses, especially SMEs, to supply digital content or digital services across the Union. They would provide businesses with a stable contract law environment when supplying digital content or digital services in other Member States. They would also prevent legal fragmentation that otherwise would arise from new national legislation regulating specifically digital content and digital services.

(8) Consumers should benefit from harmonised rights for the supply of digital content and digital services that provide a high level of protection. They should have clear mandatory rights when they receive or access digital content or digital services from anywhere in the Union. Having such rights should increase their confidence in acquiring digital content or digital services. It should also contribute to reducing the detriment consumers currently suffer, since there would be a set of clear rights that will enable them to address problems they face with digital content or digital services.

(9) This Directive should fully harmonise certain key rules that have, so far, not been regulated at Union or national level.

(10) This Directive should define its scope in a clear and unequivocal manner and provide clear substantive rules for the digital content or digital services falling within its scope. Both the scope of this Directive and its substantive rules should be technologically neutral and future-proof.

(11) This Directive should lay down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or a digital service. For this purpose, rules on the conformity of digital content or a digital service with the contract, remedies in the event of a lack of such conformity or a failure to supply and the modalities for the exercise of those remedies, as well as on the modification of digital content or a digital service, should be fully harmonised. Fully harmonised rules on some essential elements of consumer contract law would make it easier for businesses, especially SMEs, to offer their products in other Member States. Consumers would benefit from a high level of consumer protection and welfare gains by fully harmonising key rules. Member States are precluded within the scope of this Directive from providing for any further formal or substantive requirements. For example, Member States should not provide for rules on the reversal of the burden of proof that are different from those provided for in this Directive, or for an obligation for the consumer to notify the trader of a lack of conformity within a specific period.

(12) This Directive should not affect national law to the extent that the matters concerned are not regulated by this Directive, such as national rules on the formation, validity, nullity or effects of contracts or the legality of the digital content or the digital service. This Directive should also not determine the legal nature of contracts for the supply of digital content or a digital service, and the question of whether such contracts constitute, for instance, a sales, service, rental or sui generis contract, should be left to national law. This Directive should also not affect national rules that do not specifically concern consumer contracts and provide for specific remedies for certain types of defects that were not apparent at the time of conclusion of the contract, namely national provisions which may lay down specific rules for the trader's liability for hidden defects. This Directive should also not affect national laws providing for non-contractual remedies for the consumer, in the event of lack of conformity of the digital content or digital service, against persons in previous links of the chain of transactions, or other persons that fulfil the obligations of such persons.

(13) Member States also remain free, for example, to regulate liability claims of a consumer against a third party other than a trader that supplies or undertakes to supply the digital content or

digital service, such as a developer which is not at the same time the trader under this Directive.

(14) Member States should also remain free, for example, to regulate the consequences of a failure to supply, or of a lack of conformity of, digital content or a digital service, where such failure to supply or lack of conformity is due to an impediment beyond the control of the trader and where the trader could not be expected to have avoided or overcome the impediment or its consequences, such as in the event of force majeure.

(15) Member States should also remain free, for example, to regulate the rights of parties to withhold the performance of their obligations or part thereof until the other party performs its obligations. For example, Member States should be free to regulate whether a consumer, in cases of a lack of conformity, is to be entitled to withhold payment of the price or part thereof until the trader has brought the digital content or digital service into conformity, or whether the trader is to be entitled to retain any reimbursement due to the consumer upon termination of the contract until the consumer complies with the obligation provided for in this Directive to return the tangible medium to the trader.

(16) Member States should also remain free to extend the application of the rules of this Directive to contracts that are excluded from the scope of this Directive, or to otherwise regulate such contracts. For instance, Member States should remain free to extend the protection afforded to consumers by this Directive also to natural or legal persons that are not consumers within the meaning of this Directive, such as non-governmental organisations, start-ups or SMEs.

(17) The definition of a consumer should cover natural persons who are acting outside their trade, business, craft or profession. However, Member States should also remain free to determine, in the case of dual purpose contracts, where the contract is concluded for purposes that are partly within and partly outside the person's trade, and where the trade purpose is so limited as not to be predominant in the overall context of the contract, whether and under which conditions that person should also be considered a consumer.

(18) This Directive should apply to any contract whereby the trader supplies or undertakes to supply digital content or digital service to the consumer. Platform providers could be considered to be traders under this Directive if they act for purposes relating to their own business and as the direct contractual partner of the consumer for the supply of digital content or a digital service. Member States should remain free to extend the application of this Directive to platform providers that do not fulfil the requirements for being considered a trader under this Directive.

(19) The Directive should address problems across different categories of digital content, digital services, and their supply. In order to cater for fast technological developments and to maintain the future-proof nature of the notion of digital content or digital service, this Directive should cover, inter alia, computer programmes, applications, video files, audio files, music files, digital games, e-books or other e-publications, and also digital services which allow the creation of, processing of, accessing or storage of data in digital form, including software-as-a-service, such as video and audio sharing and other file hosting, word processing or games offered in the cloud computing environment and social media. As there are numerous ways for digital content or digital services to be supplied, such as transmission on a tangible medium, downloading by consumers on their devices, web-streaming, allowing access to storage capabilities of digital content or access to the use of social media, this Directive should apply independently of the medium used for the transmission of, or for giving access to, the digital content or digital service. However, this Directive should not apply to internet access services.

(20) This Directive and Directive (EU) 2019/771 of the European Parliament and of the Council [3] should complement each other. While this Directive lays down rules on certain requirements concerning contracts for the supply of digital content or digital services, Directive (EU) 2019/771 lays down rules on certain requirements concerning contracts for

the sale of goods. Accordingly, in order to meet the expectations of consumers and ensure a clear-cut and simple legal framework for traders of digital content, this Directive should also apply to digital content which is supplied on a tangible medium, such as DVDs, CDs, USB sticks and memory cards, as well as to the tangible medium itself, provided that the tangible medium serves exclusively as a carrier of the digital content. However, instead of the provisions of this Directive on the trader's obligation to supply and on the consumer's remedies for failure to supply, the provisions of Directive 2011/83/EU of the European Parliament and of the Council [4] on obligations related to the delivery of goods and remedies in the event of the failure to deliver should apply. In addition, the provisions of Directive 2011/83/EU on, for example, the right of withdrawal and the nature of the contract under which those goods are supplied, should also continue to apply to such tangible media and the digital content supplied on it. This Directive is also without prejudice to the distribution right applicable to these goods under copyright law.

(21) Directive (EU) 2019/771 should apply to contracts for the sale of goods, including goods with digital elements. The notion of goods with digital elements should refer to goods that incorporate or are inter-connected with digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions. Digital content or a digital service that is incorporated in or inter-connected with goods in that manner should fall within the scope of Directive (EU) 2019/771 if it is provided with the goods under a sales contract concerning those goods. Whether the supply of the incorporated or inter-connected digital content or digital service forms part of the sales contract with the seller should depend on the content of this contract. This should include incorporated or inter-connected digital content or digital services the supply of which is explicitly required by the contract. It should also include those sales contracts which can be understood as covering the supply of specific digital content or a specific digital service because they are normal for goods of the same type and the consumer could reasonably expect them given the nature of the goods and taking into account any public statement made by or on behalf of the seller or other persons in previous links of the chain of transactions, including the producer. If, for example, a smart TV were advertised as including a particular video application, that video application would be considered to be part of the sales contract. This should apply regardless of whether the digital content or digital service is pre-installed in the good itself or has to be downloaded subsequently on another device and is only inter-connected to the good.

For example, a smart phone could come with a standardised pre-installed application provided under the sales contract, such as an alarm application or a camera application. Another possible example is that of a smart watch. In such a case, the watch itself would be considered to be the good with digital elements, which can perform its functions only with an application that is provided under the sales contract but has to be downloaded by the consumer onto a smart phone; the application would then be the inter-connected digital element. This should also apply if the incorporated or inter-connected digital content or digital service is not supplied by the seller itself but is supplied, under the sales contract, by a third party. In order to avoid uncertainty for both traders and consumers, in the event of doubt as to whether the supply of the digital content or the digital service forms part of the sales contract, Directive (EU) 2019/771 should apply. Furthermore, ascertaining a bilateral contractual relationship, between the seller and the consumer, of which the supply of the incorporated or inter-connected digital content or digital service forms part should not be affected by the mere fact that the consumer has to consent to a licensing agreement with a third party in order to benefit from the digital content or the digital service.

(22) In contrast, if the absence of the incorporated or inter-connected digital content or digital service does not prevent the goods from performing their functions, or if the consumer concludes a contract for the supply of digital content or a digital service which does not form part of a sales contract concerning goods with digital elements, that contract should be

considered to be separate from the contract for the sale of the goods, even if the seller acts as an intermediary of that second contract with the third-party supplier, and could fall within the scope of this Directive. For instance, if the consumer downloads a game application from an app store onto a smart phone, the contract for the supply of the game application is separate from the contract for the sale of the smart phone itself. Directive (EU) 2019/771 should therefore only apply to the sales contract concerning the smart phone, while the supply of the game application could fall under this Directive, if the conditions of this Directive are met. Another example would be where it is expressly agreed that the consumer buys a smart phone without a specific operating system and the consumer subsequently concludes a contract for the supply of an operating system from a third party. In such a case, the supply of the separately bought operating system would not form part of the sales contract and therefore would not fall within the scope of Directive (EU) 2019/771, but could fall within the scope of this Directive, if the conditions of this Directive are met.

(23) Digital representations of value such as electronic vouchers or e-coupons are used by consumers to pay for different goods or services in the digital single market. Such digital representations of value are becoming important in relation to the supply of digital content or digital services, and should therefore be considered as a method of payment within the meaning of this Directive. Digital representations of value should also be understood to include virtual currencies, to the extent that they are recognised by national law. Differentiation depending on the methods of payment could be a cause of discrimination and provide an unjustified incentive for businesses to move towards supplying digital content or a digital service against digital representations of value. However, since digital representations of value have no other purpose than to serve as a method of payment, they themselves should not be considered digital content or a digital service within the meaning of this Directive.

(24) Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data. This Directive should apply to any contract where the consumer provides or undertakes to provide personal data to the trader. For example, this Directive should apply where the consumer opens a social media account and provides a name and email address that are used for purposes other than solely supplying the digital content or digital service, or other than complying with legal requirements. It should equally apply where the consumer gives consent for any material that constitutes personal data, such as photographs or posts that the consumer uploads, to be processed by the trader for marketing purposes. Member States should however remain free to determine whether the requirements for the formation, existence and validity of a contract under national law are fulfilled.

(25) Where digital content and digital services are not supplied in exchange for a price, this Directive should not apply to situations where the trader collects personal data exclusively to supply digital content or a digital service, or for the sole purpose of meeting legal requirements. Such situations can include, for instance, cases where the registration of the consumer is required by applicable laws for security and identification purposes. This

Directive should also not apply to situations where the trader only collects metadata, such as information concerning the consumer's device or browsing history, except where this situation is considered to be a contract under national law. It should also not apply to situations where the consumer, without having concluded a contract with the trader, is exposed to advertisements exclusively in order to gain access to digital content or a digital service. However, Member States should remain free to extend the application of this Directive to such situations, or to otherwise regulate such situations, which are excluded from the scope of this Directive.

(26) This Directive should apply to contracts for the development of digital content that is tailor-made to the specific requirements of the consumer including tailor-made software. This Directive should also apply to the supply of electronic files required in the context of 3D printing of goods, to the extent that such files fall under the definition of digital content or digital services within the meaning of this Directive. However, this Directive should not regulate any rights or obligations related to goods produced with the use of 3D printing technology.

(27) Given that this Directive should apply to contracts which have as their object the supply of digital content or a digital service to the consumer, it should not apply where the main subject matter of the contract is the provision of professional services, such as translation services, architectural services, legal services or other professional advice services, which are often performed personally by the trader, regardless of whether digital means are used by the trader in order to produce the output of the service or to deliver or transmit it to the consumer. Similarly, this Directive should not apply to public services, such as social security services or public registers, where the digital means are only used for transmitting or communicating the service to the consumer. This Directive should also not apply to authentic instruments and other notarial acts, regardless of whether they are performed, recorded, reproduced or transmitted by digital means.

(28) The market for number-independent interpersonal communications services, which do not connect with publicly assigned numbering resources, is rapidly evolving. In recent years, the emergence of new digital services which allow interpersonal communications over the internet, such as web-based email and online messaging services, has led more consumers to use such services. For such reasons, it is necessary to provide effective consumer protection with respect to such services. This Directive should therefore also apply to number-independent interpersonal communications services.

(29) This Directive should not apply to healthcare as defined in Directive 2011/24/EU of the European Parliament and of the Council [5]. The exclusion of 'healthcare' from the scope of this Directive should also apply to any digital content or digital service that constitutes a medical device, as defined in Council Directive 93/42/EEC [6] or 90/385/EEC [7] or Directive 98/79/EC of the European Parliament and of the Council [8], where such medical device is prescribed or provided by a health professional as defined in Directive 2011/24/EU. However, this Directive should apply to any digital content or digital service that constitutes a medical device, such as health applications, that can be obtained by the consumer without being prescribed or provided by a health professional.

(30) Union law relating to financial services contains numerous rules on consumer protection. Financial services, as defined by the law applicable to that sector, in particular in Directive 2002/65/EC of the European Parliament and of the Council [9], also cover digital content or digital services relating, or giving access, to financial services and are therefore covered by the protection of Union financial services law. Contracts relating to digital content or digital services that constitute a financial service should therefore be excluded from the scope of this Directive.

(31) This Directive should not apply to digital content or a digital service that is provided to a public audience as part of an artistic performance or other event, such as a digital

cinematographic projection or an audiovisual theatrical performance. However, this Directive should apply if digital content or a digital service is provided to a public audience by signal transmission such as digital television services.

(32) Free and open source software, where the source code is openly shared and users can freely access, use, modify and redistribute the software or modified versions thereof, can contribute to research and innovation in the market for digital content and digital services. In order to avoid imposing obstacles to such market developments, this Directive should also not apply to free and open source software, provided that it is not supplied in exchange for a price and that the consumer's personal data are exclusively used for improving the security, compatibility or interoperability of the software.

(33) Digital content or digital services are often combined with the provision of goods or other services and offered to the consumer within the same contract comprising a bundle of different elements, such as the provision of digital television and the purchase of electronic equipment. In such cases, the contract between the consumer and the trader includes elements of a contract for the supply of digital content or a digital service, but also elements of other contract types, such as sale of goods or services contracts. This Directive should only apply to the elements of the overall contract that consist of the supply of digital content or digital services. The other elements of the contract should be governed by the rules applicable to those contracts under national law or, as applicable, other Union law governing a specific sector or subject matter. Likewise, any effects that the termination of one element of the bundle contract could have on the other elements of that bundle contract should be governed by national law. However, in order to ensure consistency with the sector-specific provisions of Directive (EU) 2018/1972 of the European Parliament and of the Council [10] regulating bundle contracts, where a trader offers, within the meaning of that Directive, digital content or a digital service in combination with a number-based interpersonal communications service or an internet access service, the provisions of this Directive on the modification of digital content should not apply to the digital content or digital service element of the bundle. The relevant provisions of Directive (EU) 2018/1972 should instead apply to all elements of the bundle, including the digital content or digital service.

(34) The provisions of this Directive concerning bundle contracts should only apply to cases where the different elements of the bundle are offered by the same trader to the same consumer under a single contract. This Directive should not affect national laws governing the conditions under which a contract for the supply of digital content or digital services can be considered to be linked with or ancillary to another contract that the consumer has concluded with the same or another trader, the remedies to be exercised under each contract or the effect that the termination of one contract would have on the other contract.

(35) The commercial practice of bundling offers of digital content or digital services with the provision of goods or other services is subject to Directive 2005/29/EC of the European Parliament and of the Council [11] concerning unfair business-to-consumer commercial practices in the internal market. Such bundling is not in itself prohibited under Directive 2005/29/EC. However, it is prohibited where it is deemed unfair, following a case-by-case assessment pursuant to the criteria laid down in that Directive. Union law on competition also allows addressing tying and bundling practices, when they affect the competitive process and harm consumers.

(36) This Directive should be without prejudice to other Union law governing a specific sector or subject matter, such as telecommunications, e-commerce and consumer protection. It should also be without prejudice to Union and national law on copyright and related rights, including the portability of online content services.

(37) The pursuit of activities falling within the scope of this Directive could involve the processing of personal data. Union law provides a comprehensive framework on the protection of personal data. In particular, this Directive is without prejudice to Regulation (EU)

2016/679 [12] and Directive 2002/58/EC [13] of the European Parliament and of the Council. That framework applies to any personal data processed in connection with the contracts covered by this Directive. Consequently, personal data should only be collected or otherwise processed in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC. In the event of a conflict between this Directive and Union law on the protection of personal data, the latter should prevail.

(38) This Directive should not regulate the conditions for the lawful processing of personal data, as this question is regulated, in particular, by Regulation (EU) 2016/679. As a consequence, any processing of personal data in connection with a contract falling within the scope of this Directive is lawful only if it is in conformity with the provisions of Regulation (EU) 2016/679 relating to the legal grounds for the processing of personal data. Where processing of personal data is based on consent, in particular pursuant to point (a) of Article 6(1) of Regulation (EU) 2016/679, the specific provisions of that Regulation including those concerning the conditions for assessing whether consent is freely given apply. This Directive should not regulate the validity of the consent given. Regulation (EU) 2016/679 also contains comprehensive rights as to the erasure of data and data portability. This Directive should be without prejudice to those rights, which apply to any personal data provided by the consumer to the trader or collected by the trader in connection with any contract falling within the scope of this Directive, and when the consumer terminated the contract in accordance with this Directive.

(39) The right to erasure and the consumer's right to withdraw consent for the processing of personal data should apply fully also in connection with the contracts covered by this Directive. The right of the consumer to terminate the contract in accordance with this Directive should be without prejudice to the consumer's right under Regulation (EU) 2016/679 to withdraw any consent given to the processing of the consumer's personal data.

(40) This Directive should not regulate the consequences for the contracts covered by this Directive in the event that the consumer withdraws the consent for the processing of the consumer's personal data. Such consequences should remain a matter for national law.

(41) There are various ways for the trader to supply digital content or digital services to consumers. It is opportune to set simple and clear rules as to the modalities and the time for performing that obligation to supply which is the main contractual obligation of the trader, by making the digital content or a digital service available or accessible to the consumer. The digital content or digital service should be considered to be made available or accessible to the consumer when the digital content or digital service, or any means suitable for accessing or downloading it, has reached the sphere of the consumer and no further action is required by the trader in order to enable the consumer to use the digital content or digital service in accordance with the contract. Considering that the trader is not in principle responsible for acts or omissions of a third party which operates a physical or virtual facility, for instance an electronic platform or a cloud storage facility, that the consumer selects for receiving or storing the digital content or digital service, it should be sufficient for the trader to supply the digital content or digital service to that third party. However, the physical or virtual facility cannot be considered to be chosen by the consumer if it is under the trader's control or is contractually linked to the trader, or where the consumer selected that physical or virtual facility for receipt of the digital content or digital service but that choice was the only one offered by the trader to receive or access the digital content or digital service.

Where the physical or virtual facility cannot be considered to have been chosen by the consumer, the obligation of the trader to supply the digital content or digital service should not be considered to have been fulfilled if the digital content or digital service is supplied to the physical or virtual facility but the consumer cannot receive or access the digital content or digital service in accordance with this Directive. In those cases, the consumer should have the same remedies as would apply if the trader had failed to supply the digital content or

digital service. With regard to the time of supply, in line with market practices and technical possibilities, and in order to provide for a certain degree of flexibility, the digital content or digital service should be supplied without undue delay, unless the parties decide to agree otherwise in order to cater for other supply models.

(42) The digital content or digital service should comply with the requirements agreed between the trader and the consumer in the contract. In particular, it should comply with the description, quantity, for example the number of music files that can be accessed, quality, for example the picture resolution, language and version agreed in the contract. It should also possess the security, functionality, compatibility, interoperability and other features, as required by the contract. The requirements of the contract should include those resulting from the pre-contractual information which, in accordance with Directive 2011/83/EU, forms an integral part of the contract. Those requirements could also be set out in a service level agreement, where, under the applicable national law, such type of agreement forms part of the contractual relationship between the consumer and the trader.

(43) The notion of functionality should be understood to refer to the ways in which digital content or a digital service can be used. For instance, the absence or presence of any technical restrictions such as protection via Digital Rights Management or region coding could have an impact on the ability of the digital content or digital service to perform all its functions having regard to its purpose. The notion of interoperability relates to whether and to what extent digital content or a digital service is able to function with hardware or software that is different from those with which digital content or digital services of the same type are normally used. Successful functioning could include, for instance, the ability of the digital content or digital service to exchange information with such other software or hardware and to use the information exchanged.

(44) Given that digital content and digital services are constantly developing, traders may agree with consumers to provide updates and features as they become available. The conformity of the digital content or digital service should, therefore, also be assessed in relation to whether the digital content or service is updated in the manner that has been stipulated in the contract. Failure to supply updates that had been agreed to in the contract should be considered a lack of conformity of the digital content or digital service. Moreover, defective or incomplete updates should also be considered a lack of conformity of the digital content or digital service, given that that would mean that such updates are not performed in the manner stipulated in the contract.

(45) In order to be in conformity and to ensure that consumers are not deprived of their rights, for example in cases where the contract sets very low standards, the digital content or digital service should not only comply with the subjective requirements for conformity, but should in addition comply with the objective requirements for conformity set out in this Directive. Conformity should be assessed, inter alia, by considering the purpose for which digital content or digital services of the same type would normally be used. It should also possess the qualities and performance features which are normal for digital content or digital services of the same type and which consumers can reasonably expect, given the nature of the digital content or digital service, and taking into account any public statements on the specific characteristics of the digital content or digital service made by or on behalf of the trader or other persons in previous links of the chain of transactions.

(46) The standard of reasonableness with regard to any reference in this Directive to what can be reasonably expected by a person should be objectively ascertained, having regard to the nature and purpose of the digital content or digital service, the circumstances of the case and to the usages and practices of the parties involved. In particular, what is considered to be a reasonable time for bringing the digital content or digital service into conformity should be objectively ascertained, having regard to the nature of the lack of conformity.

(47) For the period of time that the consumer would reasonably expect, the trader should provide the consumer with updates, including security updates, in order to keep the digital content or digital service in conformity and secure. For instance, as regards digital content or digital services, the purpose of which is limited in time, the obligation to provide updates should be limited to that time, while for other types of digital content or digital service the period during which updates should be provided to the consumer could be equal to the liability period for lack of conformity or could extend beyond that period, which might be the case particularly with regard to security updates. The consumer should remain free to choose whether to install the updates provided. Where the consumer decides not to install the updates, the consumer should, however, not expect the digital content or digital service to remain in conformity. The trader should inform the consumer that the consumer's decision not to install updates which are necessary for keeping the digital content or digital service in conformity, including security updates, will affect the trader's liability for conformity of those features of the digital content or digital service which the relevant updates are supposed to maintain in conformity. This Directive should not affect obligations to provide security updates laid down in Union law or in national law.

(48) Regulation (EU) 2016/679 or any other Union law on data protection should fully apply to the processing of personal data in connection with any contract falling within the scope of this Directive. In addition, this Directive should be without prejudice to the rights, obligations and non-contractual remedies provided for by Regulation (EU) 2016/679. Facts leading to a lack of compliance with requirements provided for by Regulation (EU) 2016/679, including core principles such as the requirements for data minimisation, data protection by design and data protection by default, may, depending on the circumstances of the case, also be considered to constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity provided for in this Directive. One example could be where a trader explicitly assumes an obligation in the contract, or the contract can be interpreted in that way, which is also linked to the trader's obligations under Regulation (EU) 2016/679. In that case, such a contractual commitment can become part of the subjective requirements for conformity. A second example could be where non-compliance with the obligations under Regulation (EU) 2016/679 could, at the same time render the digital content or digital service unfit for its intended purpose and, therefore, constitute a lack of conformity with the objective requirement for conformity which requires the digital content or digital service to be fit for the purposes for which digital content or digital services of the same type would be normally used.

This would be the case, for example, if the trader of data encryption software fails to implement appropriate measures as required by Regulation (EU) 2016/679 to ensure that by design personal data are not disclosed to unauthorised recipients, thus rendering the encryption software unfit for its intended purpose which is the secure transferring of data by the consumer to their intended recipient. Finally, there could be cases where the trader's non-compliance with its obligations under Regulation (EU) 2016/679 can also constitute a lack of conformity of the digital content or digital service with the objective requirement for conformity which requires the digital content or digital service to possess the features which are normal for digital content or digital services of the same type and which the consumer can reasonably expect. For instance, if the trader of an online shopping application fails to take the measures provided for in Regulation (EU) 2016/679 for the security of processing of the consumer's personal data and as a result the consumer's credit card information is exposed to malware or spyware, that failure could also constitute a lack of conformity of the digital content or digital service within the meaning of this Directive, as the consumer would reasonably expect that an application of this type would normally possess features preventing the disclosure of payment details. Where the facts leading to non-compliance with requirements under Regulation (EU) 2016/679 also constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity as

provided for in this Directive, the consumer should be entitled to the remedies for the lack of conformity provided for by this Directive, unless the contract is already void or voidable under national law.

(49) In order to ensure sufficient flexibility, it should be possible for the parties to deviate from the objective requirements for conformity. Such a deviation should only be possible if the consumer was specifically informed about it and if the consumer accepts it separately from other statements or agreements and by way of active and unequivocal conduct. Both conditions could, for instance, be fulfilled by ticking a box, pressing a button or activating a similar function.

(50) When applying the rules of this Directive, traders should make use of standards, open technical specifications, good practices and codes of conduct, including in relation to the commonly used and machine-readable format for retrieving the content other than personal data, which was provided or created by the consumer when using the digital content or digital service, and including on the security of information systems and digital environments, whether established at international level, Union level or at the level of a specific industry sector. In this context, the Commission could call for the development of international and Union standards and the drawing up of a code of conduct by trade associations and other representative organisations that could support the uniform implementation of this Directive.

(51) Many types of digital content or digital services are supplied continuously over a period of time, such as access to cloud services. It is therefore necessary to ensure that the digital content or digital service is in conformity throughout the duration of the contract. Short-term interruptions of the supply of digital content or a digital service should be treated as instances of lack of conformity where those interruptions are more than negligible or recur. Moreover, given the frequent improvement of digital content and digital services, in particular by updates, the version of digital content or of a digital service supplied to the consumer should be the most recent one available at the time of the conclusion of the contract, unless the parties have agreed otherwise.

(52) In order to work properly, the digital content or digital service needs to be correctly integrated into the consumer's hardware and software environment. A lack of conformity of the digital content or digital service that results from an incorrect integration should be regarded as a lack of conformity of the digital content or digital service itself, where it was integrated by the trader or under its control, or by the consumer following the trader's instructions for integration, and the incorrect integration was due to shortcomings in the required integration instructions, such as incompleteness or a lack of clarity making the integration instructions difficult to use for the average consumer.

(53) Restrictions of the consumer's use of the digital content or digital service in accordance with this Directive could result from limitations imposed by the holder of intellectual property rights in accordance with intellectual property law. Such restrictions can arise from the end-user license agreement under which the digital content or digital service is supplied to the consumer. This can be the case when, for instance, an end-user licence agreement prohibits the consumer from making use of certain features related to the functionality of the digital content or digital service. Such a restriction could render the digital content or digital service in breach of the objective requirements for conformity laid down in this Directive, if it concerned features which are usually found in digital content or digital services of the same type and which the consumer can reasonably expect. In such cases, the consumer should be able to claim the remedies provided for in this Directive for the lack of conformity against the trader who supplied the digital content or digital service. The trader should only be able to avoid such liability by fulfilling the conditions for derogating from the objective requirements for conformity as laid down in this Directive, namely only if the trader specifically informs the consumer before the conclusion of the contract that a particular characteristic of the digital

content or digital service deviates from the objective requirements for conformity and the consumer has expressly and separately accepted that deviation.

(54) Legal defects are a particularly important issue in relation to digital content or digital services, which are subject to intellectual property rights. Restrictions on the consumer's use of digital content or a digital service in accordance with this Directive could be a result of a violation of third-party rights. Such violation might effectively bar the consumer from enjoying the digital content or digital service or some of its features, for instance when the consumer cannot access the digital content or digital service at all or cannot do so lawfully. That might be due to the fact that the third party rightfully compels the trader to stop infringing those rights and to discontinue offering the digital content or digital service in question or that the consumer cannot use the digital content or digital service without infringing the law. In the event of a violation of third-party rights that results in a restriction that prevents or limits the use of the digital content or digital service in accordance with the subjective and objective requirements for conformity, the consumer should be entitled to the remedies for the lack of conformity, unless national law provides for the nullity of the contract, or for its rescission, for example for breach of legal warranty against eviction.

(55) The trader should be liable to the consumer in the event of a lack of conformity of the digital content or digital service, and for any failure to supply the digital content or digital service. As digital content or digital services can be supplied to consumers through one or more individual acts of supply or continuously over a period of time, it is appropriate that the relevant time for the purpose of establishing conformity of the digital content or digital service be determined in the light of those different types of supply.

(56) Digital content or digital services can be supplied to consumers through a single act of supply, for instance when consumers download an e-book and store it on their personal device. Similarly, the supply can consist of a series of such individual acts, for instance where consumers receive a link to download a new e-book every week. The distinctive element of this category of digital content or digital service is the fact that consumers thereafter have the possibility to access and use the digital content or digital service indefinitely. In such cases, the conformity of the digital content or digital service should be assessed at the time of supply, and therefore the trader should only be liable for any lack of conformity which exists at the time when the single act of supply or each individual act of supply takes place. In order to ensure legal certainty, traders and consumers should be able to rely on a harmonised minimum period during which the trader should be held liable for a lack of conformity. In relation to contracts which provide for a single act of supply or a series of individual acts of supply of the digital content or digital service, Member States should ensure that traders are liable for not less than two years from the time of supply, if under their respective national law the trader is only liable for any lack of conformity that becomes apparent within a period of time after supply.

(57) Digital content or digital services could also be supplied to consumers in a continuous manner over a period of time. Continuous supply can include cases whereby the trader makes a digital service available to consumers for a fixed or an indefinite period of time, such as a two-year cloud storage contract or an indefinite social media platform membership. The distinctive element of this category is the fact that the digital content or digital service is available or accessible to consumers only for the fixed duration of the contract or for as long as the indefinite contract is in force. Therefore, it is justified that the trader, in such cases, should only be liable for a lack of conformity which appears during that period of time. The element of continuous supply should not necessarily require a long-term supply. Cases such as web-streaming of a video clip should be considered continuous supply over a period of time, regardless of the actual duration of the audio-visual file. Cases where specific elements of the digital content or digital service are made available periodically or on several instances during the fixed duration of the contract, or for as long as the indefinite contract is in force, should also be considered a continuous supply over a period of time, for instance where the

contract stipulates that a copy of anti-virus software can be used for a year and will be automatically updated on the first day of each month of this period, or that the trader will issue updates whenever new features of a digital game become available, and the digital content or digital service is available or accessible to consumers only for the fixed duration of the contract or for as long as the indefinite contract is in force.

(58) Member States should remain free to regulate national limitation periods. However, such limitation periods should not prevent consumers from exercising their rights throughout the period of time during which the trader is liable for a lack of conformity. While this Directive should therefore not harmonise the starting point of national limitation periods, it should nevertheless ensure that such periods still allow consumers to exercise their remedies for any lack of conformity that becomes apparent at least during the period during which the trader is liable for a lack of conformity.

(59) Due to the specific nature and high complexity of digital content and digital services, as well as the trader's better knowledge and access to know-how, technical information and high-tech assistance, the trader is likely to be in a better position than the consumer to know why the digital content or digital service is not supplied or is not in conformity. The trader is also likely to be in a better position to assess whether the failure to supply or the lack of conformity is due to the incompatibility of the consumer's digital environment with the technical requirements for the digital content or digital service. Therefore in the event of a dispute, while it is for the consumer to provide evidence that the digital content or digital service is not in conformity, the consumer should not have to prove that the lack of conformity existed at the time of supply of the digital content or digital service or, in the event of continuous supply, during the duration of the contract.

Instead, it should be for the trader to prove that the digital content or digital service was in conformity at that time or during that period. That burden of proof should be on the trader for a lack of conformity which becomes apparent within one year from the time of supply where the contract provides for a single act of supply or a series of individual acts of supply, and for the duration of the contract where the contract provides for continuous supply over a period of time. However, where the trader proves that the consumer's digital environment is not compatible with the technical requirements, of which the trader informed the consumer in a clear and comprehensible manner before the conclusion of the contract, the consumer should have the burden of proving that the lack of conformity of the digital content or digital service existed at the time of supply of the digital content or digital service where the contract provides for a single act of supply or a series of individual acts of supply or, where the contract provides for continuous supply over a period of time, for the duration of the contract.

(60) Without prejudice to the fundamental right to the protection of private life, including confidentiality of communications, and to the protection of personal data of the consumer, the consumer should cooperate with the trader in order for the trader to ascertain whether the cause of the lack of conformity lies in the consumer's digital environment using the technically available means which are least intrusive for the consumer. This can often be done for instance by providing the trader with automatically generated incident reports or with details of the consumer's internet connection. Only in exceptional and duly justified circumstances where, despite the best use of all other means, there is no other way possible, consumers may need to allow virtual access to their digital environment. However, where the consumer does not cooperate with the trader and the consumer had been informed of the consequences of non-cooperation, it should be for the consumer to prove not only that the digital content or digital service is not in conformity, but also that the digital content or digital service was not in conformity at the time of supply of the digital content or digital service where the contract provides for a single act of supply or a series of individual acts of supply or, where the contract provides for continuous supply over a period of time, for the duration of the contract.

(61) Where the trader has failed to supply the digital content or digital service, the consumer should call upon the trader to supply the digital content or digital service. In such cases, the trader should act without undue delay, or within an additional period of time as expressly agreed to by the parties. Considering that digital content or a digital service is supplied in digital form, the supply should not require, in the majority of situations, any additional time to make the digital content or digital service available to the consumer. Therefore, in such cases, the obligation of the trader to supply the digital content or digital service without undue delay should mean having to supply it immediately. If the trader then fails to supply the digital content or digital service, the consumer should be entitled to terminate the contract. In specific circumstances, such as where it is clear that the trader will not supply the digital content or digital service or where a specific time for the supply is essential for the consumer, the consumer should be entitled to terminate the contract without first calling upon the trader to supply the digital content or digital service.

(62) In the case of lack of conformity, consumers should be entitled to have the digital content or digital service brought into conformity, to have a proportionate reduction in the price, or to terminate the contract.

(63) Depending on the technical characteristics of the digital content or digital service, the trader should be allowed to select a specific way of bringing the digital content or digital service into conformity, for example by issuing updates or making a new copy of the digital content or digital service available to the consumer.

(64) Given the diversity of digital content and digital services, it is not appropriate to set fixed deadlines for the exercise of rights or the fulfilling of obligations related to digital content or digital services. Such deadlines would not take account of such diversity and could be either too short or too long, depending on the case. It is therefore more appropriate to require that digital content and digital services be brought into conformity within a reasonable time. Such requirement should not prevent the parties from agreeing on a specific time for bringing the digital content or digital service into conformity. The digital content or digital service should be brought into conformity free of any charge. In particular, the consumer should not incur any costs associated with the development of an update for the digital content or digital service.

(65) Where bringing digital content or a digital service into conformity is legally or factually impossible or where the trader refuses to bring the digital content or digital service into conformity because to do so would impose disproportionate costs on the trader, or where the trader has failed to bring the digital content or digital service into conformity within a reasonable time, free of charge and without causing significant inconvenience to the consumer, the consumer should be entitled to the remedies of price reduction or termination of the contract. In certain situations, it is justified that the consumer should be entitled to have the price reduced or the contract terminated immediately, for instance where the trader previously failed to successfully bring the digital content or digital service into conformity or where the consumer cannot be expected to maintain confidence in the ability of the trader to bring the digital content or digital service into conformity due to the serious nature of the lack of conformity. For example, the consumer should be entitled to directly request a price reduction or the termination of the contract where the consumer is supplied with anti-virus software which is itself infected with viruses and would constitute an instance of lack of conformity of such a serious nature. The same should apply where it is clear that the trader will not bring the digital content or digital service into conformity within a reasonable time or without significant inconvenience for the consumer.

(66) In a situation where the consumer is entitled to a reduction of the price paid for the digital content or digital service which is supplied over a period of time, the calculation of the price reduction should take into consideration the decrease of value of the digital content or digital

service due both to the lack of conformity and to the time during which the consumer was unable to enjoy the digital content or digital service in conformity.

(67) Where the digital content or digital service is supplied in exchange for a price, the consumer should be able to terminate the contract only if the lack of conformity is not minor. However, where the digital content or digital service is not supplied in exchange for a price but personal data are provided by the consumer, the consumer should be entitled to terminate the contract also in cases where the lack of conformity is minor, since the remedy of price reduction is not available to the consumer. In cases where the consumer pays a price and provides personal data, the consumer should be entitled to all available remedies in the event of a lack of conformity. In particular, provided all other conditions are met, the consumer should be entitled to have the digital content or digital service brought into conformity, to have the price reduced in relation to the money paid for the digital content or digital service or to have the contract terminated.

(68) Where the consumer terminates the contract, the trader should reimburse the price paid by the consumer. However, there is a need to balance the legitimate interests of consumers and traders where the digital content or digital service is supplied over a period of time and the digital content or digital service was in conformity only for part of that period. Therefore, upon termination, the consumer should only be entitled to the part of the price paid that corresponds and is in proportion to the length of time during which the digital content or digital service was not in conformity. The consumer should also be entitled to any part of the price paid in advance for any period that would have remained after the contract was terminated.

(69) Where personal data are provided by the consumer to the trader, the trader should comply with the obligations under Regulation (EU) 2016/679. Such obligations should also be complied with in cases where the consumer pays a price and provides personal data. Upon termination of the contract, the trader should also refrain from using any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader. Such content could include digital images, video and audio files and content created on mobile devices. However, the trader should be entitled to continue to use the content provided or created by the consumer in cases where such content either has no utility outside the context of the digital content or digital service supplied by the trader, only relates to the consumer's activity, has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts, or has been generated jointly by the consumer and others, and other consumers can continue to make use of it.

(70) The consumer could be discouraged from exercising remedies for a lack of conformity of digital content or a digital service if the consumer is deprived of access to content other than personal data, which the consumer provided or created through the use of the digital content or digital service. In order to ensure that the consumer benefits from effective protection in relation to the right to terminate the contract, the trader should therefore, at the request of the consumer, make such content available to the consumer following the termination of the contract.

(71) The consumer should be entitled to retrieve the content within a reasonable time, without hindrance from the trader, in a commonly used machine-readable format and free of charge, with the exception of costs generated by the consumer's own digital environment, for instance the costs of a network connection as those costs are not specifically linked to the retrieval of the content. However, the obligation of the trader to make available such content should not apply where the content only has utility within the context of using the digital content or digital service, or relates only to the consumer's activity when using the digital content or digital service or has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts. In such cases, the content does not have

significant practical use or interest for the consumer while taking into account also the interests of the trader. Moreover, the obligation of the trader to make available to the consumer, upon termination of the contract, any content that is not personal data and has been provided or created by the consumer should be without prejudice to the trader's right not to disclose certain content in accordance with applicable law.

(72) Where the contract is terminated, the consumer should not be required to pay for the use of the digital content or digital service for any period during which the digital content or a digital service was not in conformity because that would deprive the consumer of effective protection. However, the consumer should also refrain from using the digital content or digital service and from making it available to third parties, for instance by deleting the digital content or any usable copy or rendering the digital content or digital service otherwise inaccessible.

(73) The principle of the liability of the trader for damages is an essential element of contracts for the supply of digital content or digital services. Therefore, the consumer should be entitled to claim compensation for detriment caused by a lack of conformity or a failure to supply the digital content or digital service. The compensation should put the consumer as much as possible into the position in which the consumer would have been had the digital content or digital service been duly supplied and been in conformity. As such a right to damages already exists in all Member States, this Directive should be without prejudice to national rules on the compensation of consumers for harm resulting from infringement of those rules.

(74) This Directive should also address modifications, such as updates and upgrades, which are carried out by traders on the digital content or digital service which is supplied or made accessible to the consumer over a period of time. Considering the fast-evolving character of digital content and digital services, such updates, upgrades or similar modifications may be necessary and are often advantageous for the consumer. Some modifications, for instance those stipulated as updates in the contract, may form part of the contractual commitment. Other modifications can be required to fulfil the objective requirements for conformity of the digital content or digital service as set out in this Directive. Yet other modifications, which would deviate from the objective requirements for conformity and which are foreseeable at the time of conclusion of the contract, would have to be expressly agreed to by the consumer when concluding the contract.

(75) In addition to modifications aimed at maintaining conformity, the trader should be allowed under certain conditions to modify features of the digital content or digital service, provided that the contract gives a valid reason for such a modification. Such valid reasons could encompass cases where the modification is necessary to adapt the digital content or digital service to a new technical environment or to an increased number of users or for other important operational reasons. Such modifications are often to the advantage of the consumer as they improve the digital content or digital service. Consequently, the parties to the contract should be able to include clauses in the contract which allow the trader to undertake modifications. In order to balance consumer and business interests, such a possibility for the trader should be coupled with a right for the consumer to terminate the contract where such modifications negatively impact the use of or access to the digital content or digital service in more than only a minor manner. The extent to which modifications negatively impact the use of or access to the digital content or digital service by the consumer should be objectively ascertained having regard to the nature and purpose of the digital content or digital service and to the quality, functionality, compatibility and other main features which are normal for digital content or digital services of the same type. The rules provided for in this Directive concerning such updates, upgrades or similar modifications should however not concern situations where the parties conclude a new contract for the supply of the digital content or digital service, for instance as a consequence of distributing a new version of the digital content or digital service.

(76) Consumers should be informed of modifications in a clear and comprehensible manner. Where a modification negatively impacts, in more than a minor manner, the access to or use of digital content or a digital service by the consumer, the consumer should be informed in a way that allows the information to be stored on a durable medium. A durable medium should enable the consumer to store the information for as long as is necessary to protect the interests of the consumer arising from the consumer's relationship with the trader. Such media should include, in particular, paper, DVDs, CDs, USB sticks, memory cards or hard disks as well as emails.

(77) Where a modification negatively impacts, in more than a minor manner, the access or use of the digital content or digital service by the consumer, the consumer should enjoy as a result of such a modification the right to terminate the contract free of any charge. Alternatively, the trader can decide to enable the consumer to maintain access to the digital content or digital service at no additional cost, without the modification and in conformity, in which case the consumer should not be entitled to terminate the contract. However, if the digital content or digital service that the trader enabled the consumer to maintain is no longer in conformity with the subjective and the objective requirements for conformity, the consumer should be able to rely on the remedies for a lack of conformity as provided for under this Directive. Where the requirements for such a modification as laid down in this Directive are not satisfied and the modification results in a lack of conformity, the consumer's right to bring the digital content or digital service into conformity, have the price reduced or the contract terminated, as provided for under this Directive, should remain unaffected. Similarly, where, subsequent to a modification, a lack of conformity of the digital content or digital service that has not been caused by the modification arises, the consumer should continue to be entitled to rely on remedies as provided for under this Directive for the lack of conformity in relation to this digital content or digital service.

(78) The lack of conformity of the digital content or digital service as supplied to the consumer is often due to one of the transactions in a chain that links the original designer to the final trader. While the final trader should be liable towards the consumer in the event of a lack of conformity, it is important to ensure that the trader has appropriate rights vis-à-vis different persons in the chain of transactions in order to be able to cover the liability towards the consumer. Such rights should be limited to commercial transactions and they should therefore not cover situations where the trader is liable towards the consumer for the lack of conformity of digital content or a digital service that is composed of or built upon software which was supplied without the payment of a price under a free and open-source licence by a person in previous links of the chain of transactions. However, it should be for the Member States under their applicable national law to identify the persons in the chain of transactions against which the final trader can turn and the modalities and conditions of such actions.

(79) Persons or organisations regarded under national law as having a legitimate interest in protecting consumer contractual and data protection rights should be afforded the right to initiate proceedings to ensure that the national provisions transposing this Directive are applied, either before a court or before an administrative authority which is competent to decide upon complaints, or to initiate appropriate legal proceedings.

(80) Nothing in this Directive should prejudice the application of the rules of private international law, in particular Regulations (EC) No 593/2008 [14] and (EU) No 1215/2012 [15] of the European Parliament and of the Council.

(81) The Annex to Regulation (EU) 2017/2394 of the European Parliament and of the Council [16] should be amended to include a reference to this Directive so as to facilitate cross-border cooperation on enforcement of this Directive.

(82) Annex I to Directive 2009/22/EC of the European Parliament and of the Council [17] should be amended to include a reference to this Directive so as to ensure that the collective interests of consumers laid down in this Directive are protected.

(83) Consumers should be able to benefit from their rights under this Directive as soon as the corresponding national transposition measures begin to apply. Those national transposition measures should, therefore, also apply to contracts of an indefinite or fixed duration which were concluded before the application date and provide for the supply of digital content or digital services over a period of time, either continuously or through a series of individual acts of supply, but only as regards digital content or a digital service that is supplied from the date of application of the national transposition measures. However, in order to ensure a balance between the legitimate interests of consumers and traders, the national measures transposing the provisions of this Directive on the modification of the digital content or digital service and the right to redress should only apply to contracts concluded after the application date pursuant to this Directive.

(84) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents [18], Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(85) The European Data Protection Supervisor was consulted in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council [19] and delivered an opinion on 14 March 2017 [20].

(86) Since the objectives of this Directive, namely to contribute to the functioning of the internal market by tackling in a consistent manner contract law related obstacles for the supply of digital content or digital services while preventing legal fragmentation, cannot be sufficiently achieved by the Member States but can rather, by reasons of ensuring the overall coherence of the national laws through harmonised contract law rules which would also facilitate coordinated enforcement actions, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(87) This Directive respects the fundamental rights and freedoms and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union, including those enshrined in Articles 16, 38 and 47 thereof,

HAVE ADOPTED THIS DIRECTIVE:

Article 1. Subject matter and purpose

The purpose of this Directive is to contribute to the proper functioning of the internal market while providing for a high level of consumer protection, by laying down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or digital services, in particular, rules on:

— the conformity of digital content or a digital service with the contract,
— remedies in the event of a lack of such conformity or a failure to supply, and the modalities for the exercise of those remedies, and
— the modification of digital content or a digital service.

Article 2. Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'digital content' means data which are produced and supplied in digital form;

(2)'digital service' means:

(a)a service that allows the consumer to create, process, store or access data in digital form; or

(b)a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service;

(3)'goods with digital elements' means any tangible movable items that incorporate, or are inter-connected with, digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions;

(4)'integration' means the linking and incorporation of digital content or a digital service with the components of the consumer's digital environment in order for the digital content or digital service to be used in accordance with the requirements for conformity provided for by this Directive;

(5)'trader' means any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered by this Directive;

(6)'consumer' means any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft, or profession;

(7)'price' means money or a digital representation of value that is due in exchange for the supply of digital content or a digital service;

(8)'personal data' means personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679;

(9)'digital environment' means hardware, software and any network connection used by the consumer to access or make use of digital content or a digital service;

(10)'compatibility' means the ability of the digital content or digital service to function with hardware or software with which digital content or digital services of the same type are normally used, without the need to convert the digital content or digital service;

(11)'functionality' means the ability of the digital content or digital service to perform its functions having regard to its purpose;

(12)'interoperability' means the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used;

(13)'durable medium' means any instrument which enables the consumer or the trader to store information addressed personally to that person in a way that is accessible for future reference, for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored.

Article 3. Scope

1. This Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price.

This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in

accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.

2. This Directive shall also apply where the digital content or digital service is developed in accordance with the consumer's specifications.

3. With the exception of Articles 5 and 13, this Directive shall also apply to any tangible medium which serves exclusively as a carrier of digital content.

4. This Directive shall not apply to digital content or digital services which are incorporated in or inter-connected with goods within the meaning of point (3) of Article 2, and which are provided with the goods under a sales contract concerning those goods, irrespective of whether such digital content or digital service is supplied by the seller or by a third party. In the event of doubt as to whether the supply of incorporated or inter-connected digital content or an incorporated or inter-connected digital service forms part of the sales contract, the digital content or digital service shall be presumed to be covered by the sales contract.

5. This Directive shall not apply to contracts regarding:

(a) the provision of services other than digital services, regardless of whether digital forms or means are used by the trader to produce the output of the service or to deliver or transmit it to the consumer;

(b) electronic communications services as defined in point (4) of Article 2 of Directive (EU) 2018/1972, with the exception of number-independent interpersonal communications services as defined in point (7) of Article 2 of that Directive;

(c) healthcare as defined in point (a) of Article 3 of Directive 2011/24/EU;

(d) gambling services, namely, services that involve wagering a stake with pecuniary value in games of chance, including those with an element of skill, such as lotteries, casino games, poker games and betting transactions, by electronic means or any other technology for facilitating communication and at the individual request of a recipient of such services;

(e) financial services as defined in point (b) of Article 2 of Directive 2002/65/EC;

(f) software offered by the trader under a free and open-source licence, where the consumer does not pay a price and the personal data provided by the consumer are exclusively processed by the trader for the purpose of improving the security, compatibility or interoperability of that specific software;

(g) the supply of digital content where the digital content is made available to the general public other than by signal transmission as a part of a performance or event, such as digital cinematographic projections;

(h) digital content provided in accordance with Directive 2003/98/EC of the European Parliament and of the Council [21] by public sector bodies of the Member States.

6. Without prejudice to paragraph 4 of this Article, where a single contract between the same trader and the same consumer includes in a bundle elements of supply of digital content or a digital service and elements of the provision of other services or goods, this Directive shall only apply to the elements of the contract concerning the digital content or digital service.

Article 19 of this Directive shall not apply where a bundle within the meaning of Directive (EU) 2018/1972 includes elements of an internet access service as defined in point (2) of Article 2 of Regulation (EU) 2015/2120 of the European Parliament and of the Council [22] or a number-based interpersonal communications service as defined in point (6) of Article 2 of Directive (EU) 2018/1972.

Without prejudice to Article 107(2) of Directive (EU) 2018/1972, the effects that the termination of one element of a bundle contract may have on the other elements of the bundle contract shall be governed by national law.

7. If any provision of this Directive conflicts with a provision of another Union act governing a specific sector or subject matter, the provision of that other Union act shall take precedence over this Directive.

8. Union law on the protection of personal data shall apply to any personal data processed in connection with contracts referred to in paragraph 1.

In particular, this Directive shall be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC. In the event of conflict between the provisions of this Directive and Union law on the protection of personal data, the latter prevails.

9. This Directive shall be without prejudice to Union and national law on copyright and related rights, including Directive 2001/29/EC of the European Parliament and of the Council [23].

10. This Directive shall not affect the freedom of Member States to regulate aspects of general contract law, such as rules on the formation, validity, nullity or effects of contracts, including the consequences of the termination of a contract in so far as they are not regulated in this Directive, or the right to damages.

Article 4. Level of harmonisation

Member States shall not maintain or introduce, in their national law, provisions diverging from those laid down in this Directive, including more, or less, stringent provisions to ensure a different level of consumer protection, unless otherwise provided for in this Directive.

Article 5. Supply of the digital content or digital service

1. The trader shall supply the digital content or digital service to the consumer. Unless the parties have agreed otherwise, the trader shall supply the digital content or digital service without undue delay after the conclusion of the contract.

2. The trader shall have complied with the obligation to supply when:

(a) the digital content or any means suitable for accessing or downloading the digital content is made available or accessible to the consumer, or to a physical or virtual facility chosen by the consumer for that purpose;

(b) the digital service is made accessible to the consumer or to a physical or virtual facility chosen by the consumer for that purpose.

Article 6. Conformity of the digital content or digital service

The trader shall supply to the consumer digital content or a digital service that meets the requirements set out in Articles 7, 8 and 9, where applicable, without prejudice to Article 10.

Article 7. Subjective requirements for conformity

In order to conform with the contract, the digital content or digital service shall, in particular, where applicable:

(a) be of the description, quantity and quality, and possess the functionality, compatibility, interoperability and other features, as required by the contract;

(b) be fit for any particular purpose for which the consumer requires it and which the consumer made known to the trader at the latest at the time of the conclusion of the contract, and in respect of which the trader has given acceptance;

(c) be supplied with all accessories, instructions, including on installation, and customer assistance as required by the contract; and

(d) be updated as stipulated by the contract.

Article 8. **Objective requirements for conformity**

1. In addition to complying with any subjective requirement for conformity, the digital content or digital service shall:

(a) be fit for the purposes for which digital content or digital services of the same type would normally be used, taking into account, where applicable, any existing Union and national law, technical standards or, in the absence of such technical standards, applicable sector-specific industry codes of conduct;

(b) be of the quantity and possess the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity and security, normal for digital content or digital services of the same type and which the consumer may reasonably expect, given the nature of the digital content or digital service and taking into account any public statement made by or on behalf of the trader, or other persons in previous links of the chain of transactions, particularly in advertising or on labelling unless the trader shows that:

(i) the trader was not, and could not reasonably have been, aware of the public statement in question;

(ii) by the time of conclusion of the contract, the public statement had been corrected in the same way as, or in a way comparable to how, it had been made; or

(iii) the decision to acquire the digital content or digital service could not have been influenced by the public statement;

(c) where applicable, be supplied along with any accessories and instructions which the consumer may reasonably expect to receive; and

(d) comply with any trial version or preview of the digital content or digital service, made available by the trader before the conclusion of the contract.

2. The trader shall ensure that the consumer is informed of and supplied with updates, including security updates, that are necessary to keep the digital content or digital service in conformity, for the period of time:

(a) during which the digital content or digital service is to be supplied under the contract, where the contract provides for a continuous supply over a period of time; or

(b) that the consumer may reasonably expect, given the type and purpose of the digital content or digital service and taking into account the circumstances and nature of the contract, where the contract provides for a single act of supply or a series of individual acts of supply.

3. Where the consumer fails to install, within a reasonable time, updates supplied by the trader in accordance with paragraph 2, the trader shall not be liable for any lack of conformity resulting solely from the lack of the relevant update, provided that:

(a) the trader informed the consumer about the availability of the update and the consequences of the failure of the consumer to install it; and

(b) the failure of the consumer to install or the incorrect installation by the consumer of the update was not due to shortcomings in the installation instructions provided by the trader.

4. Where the contract provides for a continuous supply of digital content or digital service over a period of time, the digital content or digital service shall be in conformity throughout the duration of that period.

5. There shall be no lack of conformity within the meaning of paragraph 1 or 2 if, at the time of the conclusion of the contract, the consumer was specifically informed that a particular characteristic of the digital content or digital service was deviating from the objective requirements for conformity laid down in paragraph 1 or 2 and the consumer expressly and separately accepted that deviation when concluding the contract.

6. Unless the parties have agreed otherwise, digital content or a digital service shall be supplied in the most recent version available at the time of the conclusion of the contract.

Article 9. **Incorrect integration of the digital content or digital service**

Any lack of conformity resulting from the incorrect integration of the digital content or digital service into the consumer's digital environment shall be regarded as lack of conformity of the digital content or digital service if:

(a) the digital content or digital service was integrated by the trader or under the trader's responsibility; or

(b) the digital content or digital service was intended to be integrated by the consumer and the incorrect integration was due to shortcomings in the integration instructions provided by the trader.

Article 10. **Third-party rights**

Where a restriction resulting from a violation of any right of a third party, in particular intellectual property rights, prevents or limits the use of the digital content or digital service in accordance with Articles 7 and 8, Member States shall ensure that the consumer is entitled to the remedies for lack of conformity provided for in Article 14, unless national law provides for the nullity or rescission of the contract for the supply of the digital content or digital service in such cases.

Article 11. **Liability of the trader**

1. The trader shall be liable for any failure to supply the digital content or digital service in accordance with Article 5.

2. Where a contract provides for a single act of supply or a series of individual acts of supply, the trader shall be liable for any lack of conformity under Articles 7, 8 and 9 which exists at the time of supply, without prejudice to point (b) of Article 8(2).

If, under national law, the trader is only liable for a lack of conformity that becomes apparent within a period of time after supply, that period shall not be less than two years from the time of supply, without prejudice to point (b) of Article 8(2).

If, under national law, the rights laid down in Article 14 are also subject or only subject to a limitation period, Member States shall ensure that such limitation period allows the consumer to exercise the remedies laid down in Article 14 for any lack of conformity that exists at the time indicated in the first subparagraph and becomes apparent within the period of time indicated in the second subparagraph.

3. Where the contract provides for continuous supply over a period of time, the trader shall be liable for a lack of conformity under Articles 7, 8 and 9, that occurs or becomes apparent within the period of time during which the digital content or digital service is to be supplied under the contract.

If, under national law, the rights laid down in Article 14 are also subject or only subject to a limitation period, Member States shall ensure that such limitation period allows the consumer to exercise the remedies laid down in Article 14 for any lack of conformity that occurs or becomes apparent during the period of time referred to in the first subparagraph.

Article 12. Burden of proof

1. The burden of proof with regard to whether the digital content or digital service was supplied in accordance with Article 5 shall be on the trader.

2. In cases referred to in Article 11(2), the burden of proof with regard to whether the supplied digital content or digital service was in conformity at the time of supply shall be on the trader for a lack of conformity which becomes apparent within a period of one year from the time when the digital content or digital service was supplied.

3. In cases referred to in Article 11(3), the burden of proof with regard to whether the digital content or digital service was in conformity within the period of time during which the digital content or digital service is to be supplied under the contract shall be on the trader for a lack of conformity which becomes apparent within that period.

4. Paragraphs 2 and 3 shall not apply where the trader demonstrates that the digital environment of the consumer is not compatible with the technical requirements of the digital content or digital service and where the trader informed the consumer of such requirements in a clear and comprehensible manner before the conclusion of the contract.

5. The consumer shall cooperate with the trader, to the extent reasonably possible and necessary, to ascertain whether the cause of the lack of conformity of the digital content or digital service at the time specified in Article 11(2) or (3), as applicable, lay in the consumer's digital environment. The obligation to cooperate shall be limited to the technically available means which are least intrusive for the consumer. Where the consumer fails to cooperate, and where the trader informed the consumer of such requirement in a clear and comprehensible manner before the conclusion of the contract, the burden of proof with regard to whether the lack of conformity existed at the time specified in Article 11(2) or (3), as applicable, shall be on the consumer.

Article 13. Remedy for the failure to supply

1. Where the trader has failed to supply the digital content or digital service in accordance with Article 5, the consumer shall call upon the trader to supply the digital content or digital service. If the trader then fails to supply the digital content or digital service without undue delay, or within an additional period of time, as expressly agreed to by the parties, the consumer shall be entitled to terminate the contract.

2. Paragraph 1 shall not apply, and the consumer shall be entitled to terminate the contract immediately, where:

(a) the trader has declared, or it is equally clear from the circumstances, that the trader will not supply the digital content or digital service;

(b) the consumer and the trader have agreed, or it is clear from the circumstances attending the conclusion of the contract, that a specific time for the supply is essential for the consumer and the trader fails to supply the digital content or digital service by or at that time.

3. Where the consumer terminates the contract under paragraph 1 or 2 of this Article, Articles 15 to 18 shall apply accordingly.

Article 14. Remedies for lack of conformity

1. In the case of a lack of conformity, the consumer shall be entitled to have the digital content or digital service brought into conformity, to receive a proportionate reduction in the price, or to terminate the contract, under the conditions set out in this Article.

2. The consumer shall be entitled to have the digital content or digital service brought into conformity, unless this would be impossible or would impose costs on the trader that would be disproportionate, taking into account all the circumstances of the case including:

(a) the value the digital content or digital service would have if there were no lack of conformity; and

(b) the significance of the lack of conformity.

3. The trader shall bring the digital content or digital service into conformity pursuant to paragraph 2 within a reasonable time from the time the trader has been informed by the consumer about the lack of conformity, free of charge and without any significant inconvenience to the consumer, taking account of the nature of the digital content or digital service and the purpose for which the consumer required the digital content or digital service.

4. The consumer shall be entitled to either a proportionate reduction of the price in accordance with paragraph 5 where the digital content or digital service is supplied in exchange for a payment of a price, or the termination of the contract in accordance with paragraph 6, in any of the following cases:

(a) the remedy to bring the digital content or digital service into conformity is impossible or disproportionate in accordance with paragraph 2;

(b) the trader has not brought the digital content or digital service into conformity in accordance with paragraph 3;

(c) a lack of conformity appears despite the trader's attempt to bring the digital content or digital service into conformity;

(d) the lack of conformity is of such a serious nature as to justify an immediate price reduction or termination of the contract; or

(e) the trader has declared, or it is clear from the circumstances, that the trader will not bring the digital content or digital service into conformity within a reasonable time, or without significant inconvenience for the consumer.

5. The reduction in price shall be proportionate to the decrease in the value of the digital content or digital service which was supplied to the consumer compared to the value that the digital content or digital service would have if it were in conformity.

Where the contract stipulates that the digital content or digital service shall be supplied over a period of time in exchange for the payment of a price, the reduction in price shall apply to the period of time during which the digital content or digital service was not in conformity.

6. Where the digital content or digital service is supplied in exchange for the payment of a price, the consumer shall be entitled to terminate the contract only if the lack of conformity is not minor. The burden of proof with regard to whether the lack of conformity is minor shall be on the trader.

Article 15. Exercise of the right of termination

The consumer shall exercise the right to terminate the contract by means of a statement to the trader expressing the decision to terminate the contract.

Article 16. Obligations of the trader in the event of termination

1. In the event of termination of the contract, the trader shall reimburse the consumer for all sums paid under the contract.

However, in cases where the contract provides for the supply of the digital content or digital service in exchange for a payment of a price and over a period of time, and the digital content or digital service had been in conformity for a period of time prior to the termination of the contract, the trader shall reimburse the consumer only for the proportionate part of the price paid corresponding to the period of time during which the digital content or digital service was not in conformity, and any part of the price paid by the consumer in advance for any period of the contract that would have remained had the contract not been terminated.

2. In respect of personal data of the consumer, the trader shall comply with the obligations applicable under Regulation (EU) 2016/679.

3. The trader shall refrain from using any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader, except where such content:

(a) has no utility outside the context of the digital content or digital service supplied by the trader;

(b) only relates to the consumer's activity when using the digital content or digital service supplied by the trader;

(c) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts; or

(d) has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content.

4. Except in the situations referred to in point (a), (b) or (c) of paragraph 3, the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader.

The consumer shall be entitled to retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format.

5. The trader may prevent any further use of the digital content or digital service by the consumer, in particular by making the digital content or digital service inaccessible to the consumer or disabling the user account of the consumer, without prejudice to paragraph 4.

Article 17. Obligations of the consumer in the event of termination

1. After the termination of the contract, the consumer shall refrain from using the digital content or digital service and from making it available to third parties.

2. Where the digital content was supplied on a tangible medium, the consumer shall, at the request and at the expense of the trader, return the tangible medium to the trader without undue delay. If the trader decides to request the return of the tangible medium, that request shall be made within 14 days of the day on which the trader is informed of the consumer's decision to terminate the contract.

3. The consumer shall not be liable to pay for any use made of the digital content or digital service in the period, prior to the termination of the contract, during which the digital content or the digital service was not in conformity.

Article 18. Time limits and means of reimbursement by the trader

1. Any reimbursement that is owed to the consumer by the trader, pursuant to Article 14(4) and (5) or 16(1), due to a price reduction or termination of the contract shall be carried out without undue delay and, in any event, within 14 days of the date on which the trader is informed of the consumer's decision to invoke the consumer's right for a price reduction or to terminate the contract.

2. The trader shall carry out the reimbursement using the same means of payment as the consumer used to pay for the digital content or digital service, unless the consumer expressly agrees otherwise, and provided that the consumer does not incur any fees as a result of such reimbursement.

3. The trader shall not impose any fee on the consumer in respect of the reimbursement.

Article 19. Modification of the digital content or digital service

1. Where the contract provides that the digital content or digital service is to be supplied or made accessible to the consumer over a period of time, the trader may modify the digital content or digital service beyond what is necessary to maintain the digital content or digital service in conformity in accordance with Articles 7 and 8, if the following conditions are met:

(a) the contract allows, and provides a valid reason for, such a modification;

(b) such a modification is made without additional cost to the consumer;

(c) the consumer is informed in a clear and comprehensible manner of the modification; and

(d) in the cases referred to in paragraph 2, the consumer is informed reasonably in advance on a durable medium of the features and time of the modification and of the right to terminate the contract in accordance with paragraph 2, or of the possibility to maintain the digital content or digital service without such a modification in accordance with paragraph 4.

2. The consumer shall be entitled to terminate the contract if the modification negatively impacts the consumer's access to or use of the digital content or digital service, unless such negative impact is only minor. In that case, the consumer shall be entitled to terminate the contract free of charge within 30 days of the receipt of the information or of the time when the digital content or digital service has been modified by the trader, whichever is later.

3. Where the consumer terminates the contract in accordance with paragraph 2 of this Article, Articles 15 to 18 shall apply accordingly.

4. Paragraphs 2 and 3 of this Article shall not apply if the trader has enabled the consumer to maintain without additional cost the digital content or digital service without the modification, and the digital content or digital service remains in conformity.

Article 20. Right of redress

Where the trader is liable to the consumer because of any failure to supply the digital content or digital service, or because of a lack of conformity resulting from an act or omission by a person in previous links of the chain of transactions, the trader shall be entitled to pursue remedies against the person or persons liable in the chain of commercial transactions. The person against whom the trader may pursue remedies, and the relevant actions and conditions of exercise, shall be determined by national law.

Article 21. Enforcement

1. Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive.

2. The means referred to in paragraph 1 shall include provisions whereby one or more of the following bodies, as determined by national law, may take action under national law before the courts or before the competent administrative bodies to ensure that the national provisions transposing this Directive are applied:

(a) public bodies or their representatives;

(b) consumer organisations having a legitimate interest in protecting consumers;

(c) professional organisations having a legitimate interest in acting;

(d) not-for-profit bodies, organisations or associations, active in the field of the protection of data subjects' rights and freedoms as defined in Article 80 of Regulation (EU) 2016/679.

Article 22. Mandatory nature

1. Unless otherwise provided for in this Directive, any contractual term which, to the detriment of the consumer, excludes the application of the national measures transposing this Directive, derogates from them or varies their effects before the failure to supply or the lack of conformity is brought to the trader's attention by the consumer, or before the modification of the digital content or digital service in accordance with Article 19 is brought to the consumer's attention by the trader, shall not be binding on the consumer.

2. This Directive shall not prevent the trader from offering the consumer contractual arrangements that go beyond the protection provided for in this Directive.

Article 23. Amendments to Regulation (EU) 2017/2394 and Directive 2009/22/EC

(1) In the Annex to Regulation (EU) 2017/2394, the following point is added:

'28.Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019, p. 1)'.

(2) In Annex I to Directive 2009/22/EC, the following point is added:

'17.Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019, p. 1)'.

Article 24. Transposition

1. By 1 July 2021 Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 1 January 2022.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field covered by this Directive.

2. The provisions of this Directive shall apply to the supply of digital content or digital services which occurs from 1 January 2022 with the exception of Articles 19 and 20 of this Directive which shall only apply to contracts concluded from that date.

Article 25. Review

The Commission shall, not later than 12 June 2024 review the application of this Directive and submit a report to the European Parliament, to the Council and to the European Economic and Social Committee. The report shall examine, inter alia, the case for harmonisation of rules applicable to contracts for the supply of digital content or digital services other than that covered by this Directive, including supplied against advertisements.

Article 26. **Entry into force**

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 27. Addressees

This Directive is addressed to the Member States.
Done at Brussels, 20 May 2019.

For the European Parliament
The President
A. TAJANI
For the Council
The President
G. CIAMBA

---

(1) OJ C 264, 20.7.2016, p. 57.

(2) Position of the European Parliament of 26 March 2019 (not yet published in the Official Journal) and decision of the Council of 15 April 2019.

(3) Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 (see page 28 of this Official Journal).

(4) Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, p. 64).

(5) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(6) Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1).

(7) Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (OJ L 189, 20.7.1990, p. 17).

(8) Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices (OJ L 331, 7.12.1998, p. 1).

(9) Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC (OJ L 271, 9.10.2002, p. 16).

(10) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

(11) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the

European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

(12) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(13) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(14) Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (OJ L 177, 4.7.2008, p. 6).

(15) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

(16) Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, p. 1).

(17) Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (OJ L 110, 1.5.2009, p. 30).

(18) OJ C 369, 17.12.2011, p. 14.

(19) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(20) OJ C 200, 23.6.2017, p. 10.

(21) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

(22) Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012 (OJ L 310, 26.11.2015, p. 1).

(23) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10).

REGULATION (EU) 2019/2144 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 November 2019

on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Regulation (EU) 2018/858 of the European Parliament and of the Council (3) lays down administrative provisions and technical requirements for the type-approval of all new vehicles, systems, components and separate technical units, with a view to ensuring the proper functioning of the internal market and in order to offer a high level of safety and environmental performance.

(2) This Regulation is a regulatory act for the purposes of the EU type-approval procedure laid down by Regulation (EU) 2018/858. Therefore, Annex II to Regulation (EU) 2018/858 should be amended accordingly. The administrative provisions of Regulation (EU) 2018/858, including the provisions on corrective measures and penalties, are fully applicable to this Regulation.

(3) Over the past decades, developments in vehicle safety have contributed significantly to the overall reduction in the number of road fatalities and severe injuries. However, 25 300 people died on Union roads in 2017, a figure that has remained constant in the last four years. Moreover, 135 000 people are seriously injured in collisions every year (4). The Union should do its utmost to reduce or to eliminate accidents and injuries in road transport. In addition to safety measures to protect vehicle occupants, the implementation of specific measures to prevent fatalities and injuries of vulnerable road users, such as cyclists and pedestrians, is needed to protect road users outside of the vehicle. Without new initiatives on general road safety, the safety effects of the current approach will no longer be able to off-set the effects of increasing traffic volumes. Therefore, the safety performance of vehicles needs to be further

improved as part of an integrated road safety approach and in order to protect vulnerable road users better.

(4) Type-approval provisions should ensure that motor vehicle performance levels are assessed in a repeatable and reproducible manner. Therefore, the technical requirements in this Regulation only refer to pedestrians and cyclists, as only these presently exist as formally harmonised testing target subjects. Besides pedestrians and cyclists, vulnerable road users, in general, also include other non-motorised and motorised road users who might use personal mobility solutions without protective bodywork. Moreover, current technology creates a reasonable expectation that advanced systems will also react to other vulnerable road users under normal driving conditions, despite not being specifically tested. The technical requirements in this Regulation should be further adapted to technical progress following an assessment and review process in order to cover all road users who use personal mobility solutions without protective bodywork, such as scooters, self-balancing vehicles and wheelchairs.

(5) Technical progress in the area of advanced vehicle safety systems offers new possibilities for reducing casualty numbers. In order to minimise the number of severe injuries and fatalities, a set of new technologies needs to be introduced.

(6) Within the context of Regulation (EC) No 661/2009 of the European Parliament and of the Council (5), the Commission assessed the feasibility of extending the existing requirement in that Regulation to install certain systems (for example, advanced emergency braking systems and tyre pressure monitoring systems) in certain categories of vehicles so that it applied to all vehicle categories. The Commission also assessed the technical and economic feasibility and market maturity of imposing a new requirement to install other advanced safety features. Based on those assessments, the Commission published a report for the European Parliament and the Council on 12 December 2016 entitled 'Saving Lives: Boosting Car Safety in the EU'. The Commission Staff Working Document accompanying that report identified and put forward 19 potential regulatory measures that would be effective in further reducing the number of road accidents and road fatalities and injuries.

(7) To ensure technology neutrality, the performance requirements should allow both direct and indirect tyre pressure monitoring systems.

(8) Advanced vehicle systems can be more effective in reducing fatalities, decreasing the number of road accidents and mitigating injuries and damage if they are designed to be convenient for users. Therefore, vehicle manufacturers should do their utmost to ensure that the systems and features provided for in this Regulation are developed in such a way that supports the driver. The functioning of those systems and features and their limitations should be explained in a clear and consumer-friendly manner in the motor vehicle's user instructions.

(9) Safety features and warnings used in assisting driving should be easily perceivable by every driver, including the elderly and persons with disabilities.

(10) Advanced emergency braking systems, intelligent speed assistance, emergency lane-keeping systems, driver drowsiness and attention warning, advanced driver distraction warning and reversing detection are safety systems that have a high potential to reduce casualty numbers considerably. In addition, some of those safety systems form the basis of technologies which will also be used for the deployment of automated vehicles. Any such safety systems should function without the use of any kind of biometric information of drivers or passengers, including facial recognition. Therefore, harmonised rules and test procedures for the type-approval of vehicles as regards those systems and for the type-approval of those systems as separate technical units should be established at Union level. The technological progress of those systems should be taken into account in every evaluation of the existing legislation, in order to be future-proof, whilst strictly adhering to the principles of privacy and data

protection, and to reduce or eliminate accidents and injuries in road transport. It is also necessary to ensure that those systems can be used safely throughout the life cycle of the vehicle.

(11) It should be possible to switch off intelligent speed assistance, for instance, when a driver experiences false warnings or inappropriate feedback as a result of inclement weather conditions, temporarily conflicting road markings in construction zones, or misleading, defective or missing road signs. Such a switch-off feature should be under the control of the driver. It should allow for intelligent speed assistance to be switched off for as long as necessary and to be easily switched back on by the driver. When the system is switched off, information about the speed limit may be provided. The system should be always active when switching the ignition on and the driver should always be made aware of whether the system is on or off.

(12) It is widely recognised that safety-belts are one of the most important and effective vehicle safety features. Safety-belt reminder systems therefore have the potential to further prevent fatalities or mitigate injuries by increasing the safety-belt wearing rates across the Union. For that reason, under Regulation (EC) No 661/2009 the safety-belt reminder system was made compulsory for the driver seat in all new passenger cars from 2014 in implementation of United Nations (UN) Regulation No 16, which established the relevant technical provisions. As a result of the amendment of that UN Regulation to take account of technical progress, it is obligatory to fit all front and rear seats of M1 and N1 vehicles, as well as all front seats of N2, N3, M2 and M3 vehicles, with safety-belt reminder systems from 1 September 2019 for new types of motor vehicles and 1 September 2021 for all new motor vehicles.

(13) The introduction of event data recorders storing a range of crucial anonymised vehicle data, accompanied by requirements for data range, accuracy, resolution and for its collection, storage and retrievability over a short timeframe before, during and immediately after collision (for example, triggered by the deployment of an airbag) is a valuable step in obtaining more accurate, in-depth accident data. All motor vehicles should therefore be required to be equipped with such recorders. Those recorders should be capable of recording and storing data in such a way that the data can only be used by Member States to conduct road safety analysis and assess the effectiveness of specific measures taken without the possibility of identifying the owner or the holder of a particular vehicle on the basis of the stored data.

(14) Any processing of personal data, such as information about the driver processed in event data recorders or information about the driver's drowsiness and attention or the driver's distraction, should be carried out in accordance with with Union data protection law, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council (6). Event data recorders should operate on a closed-loop system, in which the data stored is overwritten, and which does not allow the vehicle or holder to be identified. In addition, the driver drowsiness and attention warning or advanced driver distraction warning should not continuously record nor retain any data other than what is necessary in relation to the purposes for which they were collected or otherwise processed within the closed-loop system. Furthermore, the processing of personal data collected through the 112-based eCall in-vehicle system is subject to specific safeguards set out in Regulation (EU) 2015/758 of the European Parliament and of the Council (7).

(15) Advanced emergency braking systems or emergency lane-keeping systems might not be fully operational in some cases, in particular due to shortcomings in road infrastructure. In those cases, the systems should deactivate themselves and give information about the deactivation to the driver. If they do not deactivate automatically, it should be possible to switch them off manually. Such deactivation should be temporary and should only last for the period when the system is not fully operational. Drivers might also need to override advanced emergency braking system or emergency lane keeping system where the functioning of the system could

lead to greater risk or harm. This would ensure that the vehicles are under the driver's control at all times. Nevertheless such systems could also recognise instances where the driver is incapacitated and intervention by the system is therefore needed in order to prevent an accident being worse than it would otherwise be.

(16) Regulation (EC) No 661/2009 exempted vans, sport utility vehicles (SUVs) and multi-purpose vehicles (MPVs) from safety requirements due to seating height and vehicle mass characteristics. Given the increased rate of market penetration of such vehicles (up from only 3 % in 1996 to 14 % in 2016) and the technological developments in post-crash electric safety checks, those exemptions are outdated and unjustified. Therefore, the exemptions should be removed and the whole range of advanced vehicle system requirements should be applied to those vehicles.

(17) Regulation (EC) No 661/2009 achieved significant simplification of Union legislation by replacing 38 Directives with equivalent UN Regulations that are mandatory under Council Decision 97/836/EC (8). In order to achieve further simplification, more Union rules should be replaced with existing UN Regulations that apply in the Union on a compulsory basis. Furthermore, the Commission should promote and support the on-going work at UN level in order to establish, without any delay, and in accordance with the highest road safety standards available, technical requirements for the type-approval of the vehicle safety systems provided by this Regulation.

(18) UN Regulations and the amendments thereto which the Union has voted in favour of or that the Union applies, in accordance with Decision 97/836/EC, should be incorporated within the Union type-approval legislation. Accordingly, the power should be delegated to the Commission to amend the list of UN Regulations that apply on a compulsory basis to ensure that that list is kept up-to-date.

(19) Regulation (EC) No 78/2009 of the European Parliament and of the Council (9) sets out requirements for the protection of pedestrians, cyclists and other vulnerable road users in the form of compliance tests and limit values for the type-approval of vehicles with regard to their front structure and for the type-approval of frontal protection systems (for example, bull-bars). Since the adoption of Regulation (EC) No 78/2009, technical requirements and test procedures for vehicles have developed further at UN level to take account of technical progress. UN Regulation No 127 laying down uniform provisions concerning the approval of motor vehicles with regard to their pedestrian safety performance ('UN Regulation No 127') currently also applies in the Union in respect to type-approval of motor vehicles.

(20) Following the adoption of Regulation (EC) No 79/2009 of the European Parliament and of the Council (10), the technical requirements and test procedures for the type-approval of hydrogen-powered vehicles and hydrogen systems and components, have been further developed at UN level to take account of technical progress. UN Regulation No 134 on uniform provisions concerning the approval of motor vehicles and their components with regard to the safety-related performance of hydrogen-fuelled vehicles (HFCV) (11) ('UN Regulation No 134') currently also applies in the Union in respect of type-approval of hydrogen systems in motor vehicles. In addition to those requirements, criteria for the quality of the materials and fuelling receptacles used in hydrogen vehicle systems should be established at Union level.

(21) In the interests of clarity, rationality and simplification, Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 should be repealed and replaced by this Regulation.

(22) Historically, Union rules have limited the overall length of truck combinations, which resulted in the typical cab-over-engine designs as they maximise the cargo space. However, the high position of the driver led to an increased blind-spot area and poorer direct visibility around the truck cab. This is a major factor in truck accidents involving vulnerable road users. The number of casualties could be reduced significantly by improving direct vision. Requirements

should therefore be introduced to improve direct vision to enhance the direct visibility of pedestrians, cyclists and other vulnerable road users from the driver's seat by reducing to the greatest possible extent the blind spots in front and to the side of the driver. The specificities of different categories of vehicles should be taken into account.

(23) Automated vehicles have the potential to make a huge contribution to reducing road fatalities, given that more than 90 % of road accidents are estimated to result from some level of human error. As automated vehicles will gradually take over the tasks of the driver, harmonised rules and technical requirements for automated vehicle systems, including those regarding verifiable safety assurance for decision-making by automated vehicles, should be adopted at Union level, while respecting the principle of technological neutrality, and promoted at international level in the framework of the UNECE's World Forum for Harmonization of Vehicle Regulations (WP.29).

(24) Road users such as pedestrians and cyclists, as well as drivers of non-automated vehicles that cannot receive electronic vehicle-to-vehicle information about the behaviour of an automated vehicle, should be kept informed about that behaviour by conventional means as provided for in UN Regulations or other regulatory acts as soon as possible after their entry into force.

(25) Vehicle platooning has the potential to bring about safer, cleaner and more efficient transport in the future. In anticipation of the introduction of platooning technology and the relevant standards, a regulatory framework with harmonised rules and procedures will be needed.

(26) The connectivity and automation of vehicles increase the possibility for unauthorised remote access to in-vehicle data and the illegal modification of software over the air. In order to take into account such risks, UN Regulations or other regulatory acts on cyber security should be applied on a mandatory basis as soon as possible after their entry into force.

(27) Software modifications can significantly change vehicle functionalities. Harmonised rules and technical requirements for software modifications should be established in line with the type-approval procedures. Therefore, UN Regulations or other regulatory acts regarding software update processes should be applied on a mandatory basis as soon as possible after their entry into force. However, those security measures should not compromise the obligations of the vehicle manufacturer to provide access to comprehensive diagnostic information and in-vehicle data relevant to vehicle repair and maintenance.

(28) The Union should continue to promote the development of technical requirements for tyre noise, rolling resistance and wet grip performance of tyres at the UN level. This is because UN Regulation No 117 on uniform provisions concerning the approval of tyres with regard to rolling sound emissions and/or to adhesion on wet surfaces and/or to rolling resistance (12) ('UN Regulation No 117') now contains these detailed provisions. The process of adapting the requirements on tyres to take account of technical progress should be rapidly and ambitiously continued at UN level, in particular to ensure that tyre performance is also assessed at the end of a tyre's life in its worn condition and to promote the idea that tyres should meet the requirements throughout their life and not be replaced prematurely. Existing requirements in Regulation (EC) No 661/2009 relating to tyre performance should be replaced by equivalent UN Regulations.

(29) In order to ensure the effectiveness of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission to supplement this Regulation in respect of type-approval requirements concerning advanced vehicle systems and to amend this Regulation in respect of Annex II thereof to take into account technical progress and regulatory developments. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016

on Better Law-Making (13). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(30) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (14).

(31) In view of the alignment of the Union legislation referring to the regulatory procedure with scrutiny with the legal framework introduced by the TFEU and in order to further simplify the Union legislation in the field of vehicle safety, the following Regulations should be repealed and replaced by implementing acts adopted under this Regulation:

— Commission Regulation (EC) No 631/2009 (15),

— Commission Regulation (EU) No 406/2010 (16),

— Commission Regulation (EU) No 672/2010 (17),

— Commission Regulation (EU) No 1003/2010 (18),

— Commission Regulation (EU) No 1005/2010 (19),

— Commission Regulation (EU) No 1008/2010 (20),

— Commission Regulation (EU) No 1009/2010 (21),

— Commission Regulation (EU) No 19/2011 (22),

— Commission Regulation (EU) No 109/2011 (23),

— Commission Regulation (EU) No 458/2011 (24),

— Commission Regulation (EU) No 65/2012 (25),

— Commission Regulation (EU) No 130/2012 (26),

— Commission Regulation (EU) No 347/2012 (27),

— Commission Regulation (EU) No 351/2012 (28),

— Commission Regulation (EU) No 1230/2012 (29),

— Commission Regulation (EU) 2015/166 (30).

(32) Given that EU type-approvals granted in accordance with Regulation (EC) No 78/2009, Regulation (EC) No 79/2009 or Regulation (EC) No 661/2009 and their implementing measures are to be considered equivalent to those granted in accordance with this Regulation, unless the relevant requirements are changed by this Regulation or until they are modified by the delegated acts or implementing acts adopted pursuant to this Regulation, transitional provisions are needed to ensure that such approvals are not invalidated.

(33) The dates for refusal to grant EU type-approval, refusal of vehicle registration and prohibition of the placing on the market or entry into service of components and separate technical units should be laid down for each regulated item.

(34) Since the objective of this Regulation, namely ensuring the proper functioning of the internal market through the introduction of harmonised technical requirements concerning the safety and environmental performance of motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles cannot be sufficiently

achieved by the Member States and can therefore, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(35) Detailed technical requirements and adequate test procedures, as well as provisions concerning uniform procedures and technical specifications, for type-approval of motor vehicles and their trailers, and of systems, components and separate technical units should be laid down in delegated acts and implementing acts sufficiently in advance before their date of application in order to allow enough time for manufacturers to adapt to the requirements of this Regulation and the delegated acts and implementing acts adopted pursuant to it. Some vehicles are produced in small quantities. Therefore, it is appropriate that requirements set out in this Regulation and the delegated acts and implementing acts adopted pursuant to it take into account such vehicles or classes of vehicles where such requirements are incompatible with the use or design of such vehicles, or where the additional burden imposed by them is disproportionate. Therefore, the application of this Regulation should be deferred,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1. **Subject matter**

This Regulation establishes requirements:

(a) for the type-approval of vehicles, and of systems, components and separate technical units designed and constructed for vehicles, with regard to their general characteristics and safety, and to the protection and safety of vehicle occupants and vulnerable road users;
(b) for the type-approval of vehicles, in respect of tyre pressure monitoring systems, with regard to their safety, fuel efficiency and CO2 emissions; and
(c) for the type-approval of newly-manufactured tyres with regard to their safety and environmental performance.

Article 2. Scope

This Regulation applies to vehicles of categories M, N and O, as defined in Article 4 of Regulation (EU) 2018/858, and to systems, components and separate technical units designed and constructed for such vehicles.

Article 3. Definitions

For the purposes of this Regulation, the definitions laid down in Article 3 of Regulation (EU) 2018/858 apply.

In addition, the following definitions apply:

(1) ‘vulnerable road user’ means non-motorised road users, including, in particular, cyclists and pedestrians, as well as users of powered two-wheelers;

(2)‘tyre pressure monitoring system’ means a system fitted on a vehicle which can evaluate the pressure of the tyres or the variation of pressure over time and transmit corresponding information to the user while the vehicle is running;
(3)‘intelligent speed assistance’ means a system to aid the driver in maintaining the appropriate speed for the road environment by providing dedicated and appropriate feedback;
(4)‘alcohol interlock installation facilitation’ means a standardised interface that facilitates the fitting of aftermarket alcohol interlock devices in motor vehicles;
(5)‘driver drowsiness and attention warning’ means a system that assesses the driver’s alertness through vehicle systems analysis and warns the driver if needed;
(6)‘advanced driver distraction warning’ means a system that helps the driver to continue to pay attention to the traffic situation and that warns the driver when he or she is distracted;
(7)‘emergency stop signal’ means a light-signalling function to indicate to other road users to the rear of the vehicle that a high retardation force is being applied to the vehicle relative to the prevailing road conditions;
(8)‘reversing detection’ means a system to make the driver aware of people and objects at the rear of the vehicle with the primary aim of avoiding collisions when reversing;
(9)‘lane departure warning system’ means a system to warn the driver that the vehicle is drifting out of its travel lane;
(10)‘advanced emergency braking system’ means a system which can automatically detect a potential collision and activate the vehicle braking system to decelerate the vehicle with the purpose of avoiding or mitigating a collision;
(11)‘emergency lane-keeping system’ means a system that assists the driver in keeping a safe position of the vehicle with respect to the lane or road boundary, at least when a lane departure occurs or is about to occur and a collision might be imminent;
(12)‘vehicle master control switch’ means the device by which the vehicle’s on-board electronics system is brought, from being switched off, as in the case where a vehicle is parked without the driver being present, to normal operation mode;
(13)‘event data recorder’ means a system with the only purpose of recording and storing critical crash-related parameters and information shortly before, during and immediately after a collision;
(14)‘frontal protection system’ means a separate structure or structures, such as a bull bar, or a supplementary bumper which, in addition to the original-equipment bumper, is intended to protect the external surface of the vehicle from damage in the event of a collision with an object, with the exception of structures having a mass of less than 0,5 kg, intended to protect only the vehicle’s lights;
(15)‘bumper’ means any front, lower, outer structures of a vehicle, including attachments thereto, which are intended to give protection to a vehicle when involved in a low speed frontal collision with another vehicle; it does not include however any frontal protection system;
(16)‘hydrogen-powered vehicle’ means any motor vehicle that uses hydrogen as fuel to propel the vehicle;
(17)‘hydrogen system’ means an assembly of hydrogen components and connecting parts fitted on a hydrogen-powered vehicle, excluding the hydrogen-powered propulsion system or the auxiliary power unit;
(18)‘hydrogen-powered propulsion system’ means the energy converter used to propel the vehicle;
(19)‘hydrogen component’ means hydrogen containers and all other parts of hydrogen-powered vehicles that are in direct contact with hydrogen or which form part of a hydrogen system;
(20)‘hydrogen container’ means the component within the hydrogen system that stores the primary volume of hydrogen fuel;
(21)‘automated vehicle’ means a motor vehicle designed and constructed to move autonomously for certain periods of time without continuous driver supervision but in respect of which driver intervention is still expected or required;
(22)‘fully automated vehicle’ means a motor vehicle that has been designed and constructed to move autonomously without any driver supervision;

(23)'driver availability monitoring system' means a system to assess whether the driver is in a position to take over the driving function from an automated vehicle in particular situations, where appropriate;
(24)'vehicle platooning' means the linking of two or more vehicles in a convoy using connectivity technology and automated driving support systems which allow the vehicles to maintain automatically a set, close distance between each other when connected for certain parts of a journey and to adapt to changes in the movement of the lead vehicle with little to no action from the drivers;
(25)'maximum mass' means the technically permissible maximum laden mass stated by the manufacturer;
(26)'A-pillar' means the foremost and outermost roof support extending from the chassis to the roof of the vehicle.

CHAPTER II

OBLIGATIONS OF MANUFACTURERS

Article 4. **General obligations and technical requirements**

1. Manufacturers shall demonstrate that all new vehicles that are placed on the market, registered or entered into service, and all new systems, components and separate technical units that are placed on the market or entered into service, are type-approved in accordance with the requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it.

2. Type-approval in accordance with the UN Regulations listed in Annex I shall be considered as EU type-approval in accordance with the requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it.

3. The Commission is empowered to adopt delegated acts in accordance with Article 12 to amend Annex I in order to take account of technical progress and regulatory developments by introducing and updating references to the UN Regulations, and relevant series of amendments, that apply on a compulsory basis.

4. Manufacturers shall ensure that vehicles are designed, constructed and assembled so as to minimise the risk of injury to vehicle occupants and vulnerable road users.

5. Manufacturers shall also ensure that vehicles, systems, components and separate technical units comply with the applicable requirements listed in Annex II with effect from the dates specified in that Annex, with the detailed technical requirements and test procedures laid down in the delegated acts and with the uniform procedures and technical specifications laid down in the implementing acts adopted pursuant to this Regulation, including the requirements relating to:

(a) restraint systems, crash testing, fuel system integrity and high voltage electrical safety;
(b) vulnerable road users, vision and visibility;
(c) vehicle chassis, braking, tyres and steering;
(d) on-board instruments, electrical system, vehicle lighting and protection against unauthorised use including cyberattacks;
(e) driver and system behaviour; and
(f) general vehicle construction and features.

6. The Commission is empowered to adopt delegated acts in accordance with Article 12 to amend Annex II in order to take account of technical progress and regulatory developments, in particular in relation to the matters listed in points (a) to (f) of paragraph 5 of this Article as well as those referred to in points (a) to (g) of Article 6(1), Article 7(2), (3), (4) and (5), Article 9(2), (3) and (5) and Article 11(1), and with a view to ensuring a high level of general safety of vehicles, systems, components and separate technical units and a high level of protection of vehicle occupants and vulnerable road users, by introducing and updating references to UN Regulations, as well as to delegated acts and implementing acts.

7. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for the type-approval of vehicles, systems, components and separate technical units with regard to the requirements listed in Annex II.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2). They shall be published at least 15 months before the applicable dates specified in Annex II.

Article 5. **Specific provisions relating to tyre pressure monitoring systems and tyres**

1. Vehicles shall be equipped with an accurate tyre pressure monitoring system capable, over a wide range of road and environmental conditions, of giving an in-vehicle warning to the driver when a loss of pressure occurs in a tyre.

2. Tyre pressure monitoring systems shall be designed to avoid resetting or recalibration at a low tyre pressure.

3. All tyres placed on the market shall meet the safety and environmental performance requirements set out in the relevant regulatory acts listed in Annex II.

4. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for:

(a) the type-approval of vehicles with regard to their tyre pressure monitoring systems;
(b) the type-approval of tyres, including technical specifications concerning their installation.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2). They shall be published at least 15 months before the applicable dates specified in Annex II.

Article 6. **Advanced vehicle systems for all motor vehicle categories**

1. Motor vehicles shall be equipped with the following advanced vehicle systems:

(a) intelligent speed assistance;
(b) alcohol interlock installation facilitation;
(c) driver drowsiness and attention warning;
(d) advanced driver distraction warning;
(e) emergency stop signal;
(f) reversing detection; and
(g) event data recorder.

2. Intelligent speed assistance shall meet the following minimum requirements:

(a) it shall be possible for the driver to be made aware through the accelerator control, or through dedicated, appropriate and effective feedback, that the applicable speed limit is exceeded;
(b) it shall be possible to switch off the system; information about the speed limit may still be provided, and intelligent speed assistance shall be in normal operation mode upon each activation of the vehicle master control switch;
(c) the dedicated and appropriate feedback shall be based on speed limit information obtained through the observation of road signs and signals, based on infrastructure signals or electronic map data, or both, made available in-vehicle;
(d) it shall not affect the possibility, for the drivers, of exceeding the system's prompted vehicle speed;
(e) its performance targets shall be set in order to avoid or minimise the error rate under real driving conditions.

3. Driver drowsiness and attention warning and advanced driver distraction warning systems shall be designed in such a way that those systems do not continuously record nor retain any data other than what is necessary in relation to the purposes for which they were collected or otherwise processed within the closed-loop system. Furthermore, those data shall not be accessible or made available to third parties at any time and shall be immediately deleted after processing. Those systems shall also be designed to avoid overlap and shall not prompt the driver separately and concurrently or in a confusing manner where one action triggers both systems.

4. Event data recorders shall meet the following requirements in particular:

(a) the data that they are capable of recording and storing with respect of the period shortly before, during and immediately after a collision shall include the vehicle's speed, braking, position and tilt of the vehicle on the road, the state and rate of activation of all its safety systems, 112-based eCall in-vehicle system, brake activation and relevant input parameters of the on-board active safety and accident avoidance systems, with high level of accuracy and ensured survivability of data;
(b) they cannot be deactivated;
(c) the way in which they are capable of recording and storing data shall be such that:

  (i) they operate on a closed-loop system;
  (ii) the data that they collect is anonymised and protected against manipulation and misuse; and
  (iii) the data that they collect enables precise vehicle type, variant and version, and in particular the active safety and accident avoidance systems fitted to the vehicle, to be identified; and
(d) the data that they are capable of recording can be made available to national authorities, on the basis of Union or national law, only for the purpose of accident research and analysis, including for the purposes of type approval of systems and components and in compliance with Regulation (EU) 2016/679, over a standardised interface.

5. An event data recorder shall not be capable of recording and storing the last four digits of the vehicle indicator section of the vehicle identification number or any other information which could allow the individual vehicle itself, its owner or holder, to be identified.

6. The Commission shall adopt delegated acts in accordance with Article 12 supplementing this Regulation by laying down detailed rules concerning the specific test procedures and technical requirements for:

(a) the type-approval of vehicles with regard to the advanced vehicle systems listed in paragraph 1;

(b) the type-approval of the advanced vehicle systems listed in points (a), (f) and (g) of paragraph 1 as separate technical units.

Those delegated acts shall be published at least 15 months before the applicable dates specified in Annex II.

Article 7. **Specific requirements relating to passenger cars and light commercial vehicles**

1. In addition to the other requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it that are also applicable to vehicles of categories M1 and N1, vehicles of those categories shall meet the requirements set out in paragraphs 2 to 5 and the technical specifications set out in the implementing acts referred to in paragraph 6.

2. Vehicles of categories M1 and N1 shall be equipped with advanced emergency braking systems designed and fitted in two phases and providing for:

(a) the detection of obstacles and moving vehicles ahead of the motor vehicle in the first phase;
(b) extending the detection capability referred to in point (a) to also include pedestrians and cyclists ahead of the motor vehicle in the second phase.

3. Vehicles of categories M1 and N1 shall also be equipped with an emergency lane-keeping system.

4. Advanced emergency braking systems and emergency lane-keeping systems shall meet the following requirements in particular:

(a) it shall only be possible to switch off such systems one at a time by a sequence of actions to be carried out by the driver;
(b) the systems shall be in normal operation mode upon each activation of the vehicle master control switch;
(c) it shall be possible to easily suppress audible warnings, but such action shall not at the same time suppress system functions other than audible warnings;
(d) it shall be possible for the driver to override such systems.

5. Vehicles of categories M1 and N1 shall be designed and constructed to provide for an enlarged head impact protection zone with the aim of enhancing the protection of vulnerable road users and mitigating their potential injuries in the event of a collision.

6. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for the type-approval of vehicles with regard to the requirements laid down in paragraphs 2 to 5 of this Article.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2). They shall be published at least 15 months before the applicable dates specified in Annex II.

Article 8. **Frontal protection systems for passenger cars and light commercial vehicles**

1. Frontal protection systems, whether fitted as original equipment to vehicles of categories M1 and N1 or made available on the market as separate technical units for such vehicles, shall comply with the requirements laid down in paragraph 2 and with the technical specifications set out in the implementing acts referred to in paragraph 3.

2. Frontal protection systems made available on the market as separate technical units shall be accompanied by a detailed list of the vehicle types, variants and versions for which the frontal protection system is type-approved, as well as by clear assembly instructions.

3. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for the type-approval of frontal protection systems, including technical specifications concerning their construction and installation.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2). They shall be published at least 15 months before the applicable dates specified in Annex II.

Article 9. **Specific requirements relating to buses and trucks**

1. In addition to the other requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it that are also applicable to vehicles of categories M2, M3, N2 and N3, vehicles of those categories shall meet the requirements laid down in paragraphs 2 to 5 and the technical specifications set out in the implementing acts referred to in paragraph 7. Vehicles of categories M2 and M3, shall also meet the requirement laid down in paragraph 6.

2. Vehicles of categories M2, M3, N2 and N3 shall be equipped with a lane departure warning system and an advanced emergency braking system, both of which shall comply with the the technical specifications set out in the implementing acts referred to in paragraph 7.

3. Vehicles of categories M2, M3, N2 and N3 shall be equipped with advanced systems that are capable of detecting pedestrians and cyclists located in close proximity to the front or nearside of the vehicle and of providing a warning or avoiding collision with such vulnerable road users.

4. With respect of systems referred to in paragraphs 2 and 3, they shall meet the following requirements in particular:

(a) it shall only be possible to switch off such systems one at a time by a sequence of actions to be carried out by the driver;
(b) the systems shall be in normal operation mode upon each activation of the vehicle master control switch;
(c) it shall be possible to easily suppress audible warnings, but such action shall not at the same time suppress system functions other than audible warnings;
(d) it shall be possible for the driver to override such systems.

5. Vehicles of categories M2, M3, N2 and N3 shall be designed and constructed to enhance the direct visibility of vulnerable road users from the driver seat, by reducing to the greatest possible extent the blind spots in front of and to the side of the driver, while taking into account the specificities of different categories of vehicles.

6. Vehicles of categories M2 and M3 with a capacity exceeding 22 passengers in addition to the driver and constructed with areas for standing passengers to allow frequent passenger movement shall be designed and constructed to be accessible by persons with reduced mobility, including wheelchair users.

7. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for:

(a) the type-approval of vehicles with regard to the requirements laid down in paragraphs 2 to 5 of this Article;
(b) the type-approval of the systems referred to in paragraph 3 of this Article as separate technical units.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2).

Where those implementing acts concern the requirements laid down in paragraphs 2, 3 and 4 of this Article, they shall be published at least 15 months before the applicable dates specified in Annex II.

Where those implementing acts concern the requirements laid down in paragraph 5 of this Article, they shall be published at least 36 months before the applicable dates specified in Annex II.

Article 10. **Specific requirements relating to hydrogen-powered vehicles**

1. In addition to the other requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it that are also applicable to vehicles of categories M and N, hydrogen-powered vehicles of those categories, their hydrogen systems and components of such systems shall comply with the technical specifications set out in the implementing acts referred to in paragraph 3.

2. Manufacturers shall ensure that hydrogen systems and hydrogen components are installed in accordance with the technical specifications set out in the implementing acts referred to in paragraph 3. Manufacturers shall also make available, if necessary information for the purposes of inspection of hydrogen systems and components during the service life of hydrogen-powered vehicles.

3. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for the type-approval of hydrogen-powered vehicles with regard to their hydrogen systems, including those with regard to material compatibility and fuelling receptacles, and for the type-approval of hydrogen components, including technical specifications for their installation.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2). They shall be published at least 15 months before the applicable dates specified in Annex II.

Article 11. **Specific requirements relating to automated vehicles and fully automated vehicles**

1. In addition to the other requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it that are applicable to vehicles of the respective categories, automated vehicles and fully automated vehicles shall comply with the technical specifications set out in the implementing acts referred to in paragraph 2 that relate to:

(a) systems to replace the driver's control of the vehicle, including signalling, steering, accelerating and braking;
(b) systems to provide the vehicle with real-time information on the state of the vehicle and the surrounding area;
(c) driver availability monitoring systems;
(d) event data recorders for automated vehicles;

(e) harmonised format for the exchange of data for instance for multi-brand vehicle platooning;
(f) systems to provide safety information to other road users.

However, those technical specifications relating to driver availability monitoring systems, referred to in point (c) of the first subparagraph, shall not apply to fully automated vehicles.

2. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for the systems and other items listed in points (a) to (f) of paragraph 1 of this Article, and for the type-approval of automated and fully automated vehicles with regard to those systems and other items in order to ensure the safe operation of automated and fully automated vehicles on public roads.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2).

CHAPTER III

FINAL PROVISIONS

Article 12. **Exercise of the delegation**

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 4(3) and (6) and Article 6(6) shall be conferred on the Commission for a period of five years from 5 January 2020. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 4(3) and (6) and Article 6(6) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted under Article 4(3) and (6) and Article 6(6) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 13. Committee procedure

1. The Commission shall be assisted by the Technical Committee — Motor Vehicles (TCMV). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 14. Review and reporting

1. By 7 July 2027 and every five years thereafter, the Commission shall submit an evaluation report to the European Parliament and to the Council on the achievements of the safety measures and systems, including their penetration rates and convenience for the user. The Commission shall investigate whether those safety measures and systems act as intended by this Regulation. Where appropriate, that report shall be accompanied by recommendations, including a legislative proposal to amend the requirements concerning general safety and the protection and safety of vehicle occupants and vulnerable road users, in order to further reduce or to eliminate accidents and injuries in road transport.

In particular, the Commission shall evaluate the reliability and efficiency of new intelligent speed assistance systems and the accuracy and error rate of such systems under real driving conditions. Where appropriate, the Commission shall present a legislative proposal.

2. By 31 January of each year, for the previous year, the Commission shall submit to the European Parliament and to the Council a report on the activities of the UNECE's World Forum for Harmonization of Vehicle Regulations (WP.29) as regards the progress made in the implementation of vehicle safety standards with regard to the requirements set out in Articles 5 to 11 and as regards the position of the Union related to these matters.

Article 15. Transitional provisions

1. This Regulation shall not invalidate any EU type-approvals granted to vehicles, systems, components or separate technical units which were granted in accordance with Regulation (EC) No 78/2009, Regulation (EC) No 79/2009 or Regulation (EC) No 661/2009 and their implementing measures, by 5 July 2022, unless the relevant requirements applying to such vehicles, systems, components or separate technical units have been modified, or new requirements have been added, by this Regulation and the delegated acts adopted pursuant to it, as further specified in the implementing acts adopted pursuant to this Regulation.

2. Approval authorities shall continue to grant extensions of EU type-approvals referred to in paragraph 1.

3. By way of derogation from this Regulation, Member States shall continue to permit until the date specified in Annex IV the registration of vehicles, as well as the sale or entry into service of components, which do not comply with the requirements of UN Regulation No 117.

Article 16. Implementation dates

With respect to vehicles, systems, components and separate technical units, national authorities shall:

(a) with effect from the dates specified in Annex II, with respect to a particular requirement listed in that Annex, refuse, on grounds relating to that requirement, to grant EU type-approval or national type-approval to any new type of vehicle, system, component or separate technical unit that does not comply with the requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it;
(b) with effect from the dates specified Annex II, with respect to a particular requirement listed in that Annex, consider, on grounds relating to that requirement, certificates of conformity in respect to new vehicles to be no longer valid for the purposes of Article 48 of Regulation (EU) 2018/858, and prohibit the registration of such vehicles, if those vehicles do not comply with the requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it;
(c) with effect from the dates specified in Annex II, with respect to a particular requirement listed in that Annex, prohibit, on grounds relating to that requirement, the placing on the market or entry into service of components and separate technical units, where they do not comply with the requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it.

Article 17. Amendments to Regulation (EU) 2018/858

Annex II to Regulation (EU) 2018/858 is amended in accordance with Annex III to this Regulation.

Article 18. Repeal

1. Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 and Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 are repealed with effect from the date of application of this Regulation.

2. References to Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 shall be construed as references to this Regulation.

Article 19. Entry into force and date of application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 6 July 2022.

However, Article 4(3), (6) and (7), Article 5(4), Article 6(6), Article 7(6), Article 8(3), Article 9(7), Article 10(3), Article 11(2) and Articles 12 and 13 shall apply from 5 January 2020.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 27 November 2019.

For the European Parliament

The President

D. M. SASSOLI

For the Council

The President

T. TUPPURAINEN

(1) OJ C 440, 6.12.2018, p. 90.

(2) Position of the European Parliament of 16 April 2019 (not yet published in the Official Journal) and decision of the Council of 8 November 2019.

(3) Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

(4) https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/vademecum_2018.pdf

(5) Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 200, 31.7.2009, p. 1).

(6) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(7) Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC (OJ L 123, 19.5.2015, p. 77).

(8) Council Decision 97/836/EC of 27 November 1997 with a view to accession by the European Community to the Agreement of the United Nations Economic Commission for Europe concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted to and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions ('Revised 1958 Agreement') (OJ L 346, 17.12.1997, p. 78).

(9) Regulation (EC) No 78/2009 of the European Parliament and of the Council of 14 January 2009 on the type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users, amending Directive 2007/46/EC and repealing Directives 2003/102/EC and 2005/66/EC (OJ L 35, 4.2.2009, p. 1).

(10) Regulation (EC) No 79/2009 of the European Parliament and of the Council of 14 January 2009 on type-approval of hydrogen-powered motor vehicles, and amending Directive 2007/46/EC (OJ L 35, 4.2.2009, p. 32).

(11) OJ L 129, 17.5.2019, p. 43.

(12) OJ L 218, 12.8.2016, p. 1.

(13) OJ L 123, 12.5.2016, p. 1.

(14) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(15) Commission Regulation (EC) No 631/2009 of 22 July 2009 laying down detailed rules for the implementation of Annex I to Regulation (EC) No 78/2009 of the European Parliament and of the Council on the type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users, amending Directive 2007/46/EC and repealing Directives 2003/102/EC and 2005/66/EC (OJ L 195, 25.7.2009, p. 1).

(16) Commission Regulation (EU) No 406/2010 of 26 April 2010 implementing Regulation (EC) No 79/2009 of the European Parliament and of the Council on type-approval of hydrogen-powered motor vehicles (OJ L 122, 18.5.2010, p. 1).

(17) Commission Regulation (EU) No 672/2010 of 27 July 2010 concerning type-approval requirements for windscreen defrosting and demisting systems of certain motor vehicles and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 196, 28.7.2010, p. 5).

(18) Commission Regulation (EU) No 1003/2010 of 8 November 2010 concerning type-approval requirements for the space for mounting and the fixing of rear registration plates on motor vehicles and their trailers and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 291, 9.11.2010, p. 22).

(19) Commission Regulation (EU) No 1005/2010 of 8 November 2010 concerning type-approval requirements for motor vehicle towing devices and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 291, 9.11.2010, p. 36).

(20) Commission Regulation (EU) No 1008/2010 of 9 November 2010 concerning type-approval requirements for windscreen wiper and washer systems of certain motor vehicles and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 292, 10.11.2010, p. 2).

(21) Commission Regulation (EU) No 1009/2010 of 9 November 2010 concerning type-approval requirements for wheel guards of certain motor vehicles and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 292, 10.11.2010, p. 21).

(22) Commission Regulation (EU) No 19/2011 of 11 January 2011 concerning type-approval requirements for the manufacturer's statutory plate and for the vehicle identification number of motor vehicles and their trailers and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 8, 12.1.2011, p. 1).

(23) Commission Regulation (EU) No 109/2011 of 27 January 2011 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council as regards type-approval requirements for certain categories of motor vehicles and their trailers as regards spray suppression systems (OJ L 34, 9.2.2011, p. 2).

(24) Commission Regulation (EU) No 458/2011 of 12 May 2011 concerning type-approval requirements for motor vehicles and their trailers with regard to the installation of their tyres and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council

concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 124, 13.5.2011, p. 11).

(25) Commission Regulation (EU) No 65/2012 of 24 January 2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council as regards gear shift indicators and amending Directive 2007/46/EC of the European Parliament and of the Council (OJ L 28, 31.1.2012, p. 24).

(26) Commission Regulation (EU) No 130/2012 of 15 February 2012 concerning type-approval requirements for motor vehicles with regard to vehicle access and manoeuvrability and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 43, 16.2.2012, p. 6).

(27) Commission Regulation (EU) No 347/2012 of 16 April 2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems (OJ L 109, 21.4.2012, p. 1).

(28) Commission Regulation (EU) No 351/2012 of 23 April 2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council as regards type-approval requirements for the installation of lane departure warning systems in motor vehicles (OJ L 110, 24.4.2012, p. 18).

(29) Commission Regulation (EU) No 1230/2012 of 12 December 2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with regard to type-approval requirements for masses and dimensions of motor vehicles and their trailers and amending Directive 2007/46/EC of the European Parliament and of the Council (OJ L 353, 21.12.2012, p. 31).

(30) Commission Regulation (EU) 2015/166 of 3 February 2015 supplementing and amending Regulation (EC) No 661/2009 of the European Parliament and of the Council as regards the inclusion of specific procedures, assessment methods and technical requirements, and amending Directive 2007/46/EC of the European Parliament and of the Council, and Commission Regulations (EU) No 1003/2010, (EU) No 109/2011 and (EU) No 458/2011 (OJ L 28, 4.2.2015, p. 3).

Regulation on civil aviation

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance)

(...)

CHAPTER I

PRINCIPLES

Article 1. **Subject matter and objectives**

1. The principal objective of this Regulation is to establish and maintain a high uniform level of civil aviation safety in the Union.

2. This Regulation further aims to:

(a) contribute to the wider Union aviation policy and to the improvement of the overall performance of the civil aviation sector;

(b) facilitate, in the fields covered by this Regulation, the free movement of goods, persons, services and capital, providing a level playing field for all actors in the internal aviation market, and improve the competitiveness of the Union's aviation industry;

(c) contribute to a high, uniform level of environmental protection;

(d) facilitate, in the fields covered by this Regulation, the movement of goods, services and personnel worldwide, by establishing appropriate cooperation with third countries and their aviation authorities, and by promoting the mutual acceptance of certificates and other relevant documents;

(e) promote cost-efficiency, by, inter alia, avoiding duplication, and promoting effectiveness in regulatory, certification and oversight processes as well as an efficient use of related resources at Union and national level;

(f) contribute, in the fields covered by this Regulation, to establishing and maintaining a high uniform level of civil aviation security;

(g) assist Member States, in the fields covered by this Regulation, in exercising their rights and fulfilling their obligations under the Chicago Convention, by ensuring a common interpretation and a uniform and timely implementation of its provisions, as appropriate;

(h) promote, worldwide, the views of the Union regarding civil aviation standards and civil aviation rules, by establishing appropriate cooperation with third countries and international organisations;

(i) promote research and innovation, inter alia, in regulatory, certification and oversight processes;

(j) promote, in the fields covered by this Regulation, technical and operational interoperability and the sharing of administrative best practices;

(k) support passenger confidence in a safe civil aviation.

3. The objectives set out in paragraphs 1 and 2 shall be achieved by, inter alia:

(a) the preparation, adoption and uniform application of all necessary acts;

(b) the taking of measures to improve safety standards;

(c) ensuring that the declarations and certificates issued in accordance with this Regulation, and with the delegated and implementing acts adopted on the basis thereof, are valid and recognised throughout the Union, without any additional requirements;

(d) the development, with the involvement of standardisation and other industry bodies, of detailed technical standards to be used as a means of compliance with this Regulation, and with the delegated and implementing acts adopted on the basis thereof, where appropriate;

(e) the establishment of an independent European Union Aviation Safety Agency (the 'Agency');

(f) the uniform implementation of all necessary acts by the national competent authorities and the Agency, within their respective areas of responsibility;

(g) the gathering, analysis and exchange of information to support evidence-based decision making;

(h) the undertaking of awareness and promotion initiatives, including training, communication and dissemination of relevant information.

Article 2. Scope

1. This Regulation shall apply to:

(a) the design and production of products, parts and equipment to control aircraft remotely by a natural or legal person under the oversight of the Agency or a Member State, to the extent not covered by point (b);

(b) the design, production, maintenance and operation of aircraft, as well as their engines, propellers, parts, non-installed equipment and equipment to control aircraft remotely, where the aircraft is or will be:

  (i) registered in a Member State, unless and to the extent that the Member State has transferred its responsibilities pursuant to the Chicago Convention to a third country and the aircraft is operated by a third country aircraft operator;

  (ii) registered in a third country and operated by an aircraft operator established, residing or with a principal place of business in the territory to which the Treaties apply;

  (iii) an unmanned aircraft, that is registered neither in a Member State nor in a third country and that is operated within the territory to which the Treaties apply by an aircraft operator established, residing or with a principal place of business within that territory;

(c) the operation of aircraft into, within, or out of the territory to which the Treaties apply by a third country aircraft operator;

(d) the design, production, maintenance and operation of safety-related aerodrome equipment used or intended for use at the aerodromes referred to in point (e) and the provision of groundhandling services and AMS at those aerodromes;

(e) the design, maintenance and operation of aerodromes, including the safety-related equipment used at those aerodromes, located in the territory to which the Treaties apply, which:

  (i) are open to public use;

  (ii) serve commercial air transport; and

  (iii) have a paved instrument runway of 800 metres or more, or exclusively serve helicopters using instrument approach or departure procedures;

(f) without prejudice to Union and national law on environment and land-use planning, the safeguarding of surroundings of the aerodromes referred to in point (e);

(g) the provision of ATM/ANS in the Single European Sky airspace, and the design, production, maintenance and operation of systems and constituents used in the provision of those ATM/ANS;

(h) without prejudice to Regulation (EC) No 551/2004 of the European Parliament and of the Council ([32]) and the responsibilities of Member States with regard to airspace under their jurisdiction, the design of airspace structures in the Single European Sky airspace.

2. This Regulation shall also apply to the personnel and organisations involved in the activities referred to in paragraph 1.

3. This Regulation shall not apply to:

(a) aircraft, and their engines, propellers, parts, non-installed equipment and equipment to control aircraft remotely, while carrying out military, customs, police, search and rescue, firefighting, border control, coastguard or similar activities or services under the control and responsibility of a Member State, undertaken in the public interest by or on behalf of a body vested with the powers of a public authority, and the personnel and organisations involved in the activities and services performed by those aircraft;

(b) aerodromes or parts thereof, as well as equipment, personnel and organisations, that are controlled and operated by the military;

(c) ATM/ANS, including systems and constituents, personnel and organisations, that are provided or made available by the military;

(d) the design, production, maintenance and operation of aircraft the operation of which involves low risk for aviation safety, as listed in Annex I, and to the personnel and organisations involved therein, unless the aircraft has been issued, or has been deemed to have been issued, with a certificate in accordance with Regulation (EC) No 216/2008.

As regards point (a), Member States shall ensure that activities and services performed by the aircraft referred to in that point are carried out with due regard to the safety objectives of this Regulation. Member States shall also ensure that, where appropriate, those aircraft are safely separated from other aircraft.

Without prejudice to the obligations of Member States under the Chicago Convention, aircraft covered by Annex I to this Regulation and registered in a Member State may be operated in other Member States, subject to the agreement of the Member State in the territory of which the operation takes place. Such aircraft may also be maintained, and their design may be modified, in other Member States, provided that such design modifications and such maintenance activities are carried out under the oversight of the Member State where the aircraft is registered and in accordance with procedures established by the national law of that Member State.

4. By derogation from point (d) of the first subparagraph of paragraph 3, this Regulation, and the delegated and implementing acts adopted on the basis thereof, shall apply to the design, production and maintenance of an aircraft type falling within the scope of points (e), (f), (g), (h), or (i) of point 1 of Annex I and to the personnel and organisations involved in those activities, where:

(a) the organisation responsible for the design of that aircraft type has applied for a type certificate to the Agency in accordance with Article 11 or, if applicable, has made a declaration to the Agency in accordance with point (a) of Article 18(1) in respect of that aircraft type;

(b) that aircraft type is intended for serial production; and

(c) the design of that aircraft type has not been previously approved in accordance with the national laws of a Member State.

This Regulation, and the delegated and implementing acts adopted on the basis thereof, shall apply with respect to the aircraft type concerned from the date on which the type certificate is issued or, if applicable, from the date on which the declaration is made. However, the provisions regarding the assessment of the application for the type certificate and the issuance of the type certificate by the Agency shall apply from the date at which the application is received.

5. Without prejudice to national security and defence requirements, and Article 7(5) of Regulation (EC) No 550/2004 of the European Parliament and of the Council ([33]), Member States shall ensure that:

(a) the facilities referred to in point (b) of the first subparagraph of paragraph 3 of this Article that are open to public use; and

(b) the ATM/ANS referred to in point (c) of the first subparagraph of paragraph 3 of this Article that are provided to air traffic to which Regulation (EC) No 549/2004 applies,

offer a level of safety and interoperability with civil systems that is as effective as that resulting from the application of the essential requirements set out in Annexes VII and VIII to this Regulation.

6. A Member State may decide to apply any, or any combination, of Section I, II, III, or VII of Chapter III, to some or all activities referred to in point (a) of the first subparagraph of paragraph 3 and to the personnel and organisations involved in those activities, where it considers that, in light of the characteristics of the activities, personnel and organisations in question and the purpose and content of the provisions concerned, those provisions can be effectively applied.

From the date specified in that decision, the activities, personnel and organisations concerned shall be solely regulated by the provisions of the Section, or Sections, concerned and by the provisions of this Regulation related to the application of those sections.

The Member State concerned shall without delay notify the Commission and the Agency of its decision and shall provide them with all relevant information, in particular:

(a) the Section or Sections concerned;

(b) the activities, personnel and organisations concerned;

(c) the reasons for its decision; and

(d) the date from which that decision applies.

Where the Commission, after consulting the Agency, considers that the condition specified in the first subparagraph has not been met, the Commission shall adopt implementing acts setting out its decision to that effect. Upon notification of such implementing acts to the Member State concerned, that Member State shall without delay take a decision to modify or revoke the earlier decision referred to in the first subparagraph of this paragraph and shall inform the Commission and the Agency thereof.

Without prejudice to the fourth subparagraph, a Member State may also at any time decide to modify or revoke the earlier decision referred to in the first subparagraph of this paragraph. In such cases, it shall without delay inform the Commission and the Agency thereof.

The Agency shall include in the repository referred to in Article 74 all of the decisions of the Commission and of the Member States that have been notified pursuant to this paragraph.

The Commission, the Agency and the competent authorities of the Member State concerned shall cooperate for the purpose of the application of this paragraph.

7. Member States may decide to exempt from this Regulation the design, maintenance and operation of an aerodrome, and the safety-related equipment used at that aerodrome, where that aerodrome handles no more than 10 000 commercial air transport passengers per year and no more than 850 movements related to cargo operations per year, and provided that Member States

concerned ensure that such exemption does not endanger compliance with the essential requirements referred to in Article 33.

From the date specified in that exemption decision, the design, maintenance and operation of the aerodrome concerned and the safety-related equipment and groundhandling services and AMS at that aerodrome shall no longer be regulated by this Regulation and by the delegated and implementing acts adopted on the basis thereof.

The Member State concerned shall, without delay, notify the Commission and the Agency of its exemption decision and the reasons for the adoption thereof.

Where the Commission, after consulting the Agency, considers that such exemption by a Member State does not comply with the conditions specified in the first subparagraph, the Commission shall adopt implementing acts setting out its decision to that effect. Upon notification of such implementing acts to a Member State concerned, that Member State shall without delay modify or revoke its exemption decision and shall inform the Commission and the Agency thereof.

The Member States shall also notify to the Commission and the Agency the exemptions which they have granted pursuant to Article 4(3b) of Regulation (EC) No 216/2008.

Member States shall, on an annual basis, examine the traffic figures of the aerodromes that they have exempted pursuant to this paragraph or Article 4(3b) of Regulation (EC) No 216/2008. Where that examination demonstrates that, over three consecutive years, one of those aerodromes handles more than 10 000 commercial air transport passengers per year or more than 850 movements related to cargo operations per year, the Member State concerned shall revoke the exemption of that aerodrome. In that case, it shall inform the Commission and the Agency accordingly.

The Agency shall include in the repository referred to in Article 74 all of the decisions of the Commission and of the Member States that have been notified pursuant to this paragraph.

8. A Member State may decide to exempt from this Regulation the design, production, maintenance and operation activities in respect of one or more of the following categories of aircraft:

(a) aeroplanes, other than unmanned aeroplanes, which have no more than two seats, measurable stall speed or minimum steady flight speed in landing configuration not exceeding 45 knots calibrated air speed and a maximum take-off mass (MTOM), as recorded by the Member State, of no more than 600 kg for aeroplanes not intended to be operated on water or 650 kg for aeroplanes intended to be operated on water;

(b) helicopters, other than unmanned helicopters, which have no more than two seats and a MTOM, as recorded by the Member State, of no more than 600 kg for helicopters not intended to be operated on water or 650 kg for helicopters intended to be operated on water;

(c) sailplanes, other than unmanned sailplanes, and powered sailplanes, other than unmanned powered sailplanes, which have no more than two seats and a MTOM, as recorded by the Member State, of no more than 600 kg.

However, as regards the categories of aircraft referred to in the first subparagraph Member States may not take such a decision concerning aircraft in respect of which a certificate has been issued, or has been deemed to have been issued, in accordance with Regulation (EC) No 216/2008 or with this Regulation, or in respect of which a declaration has been made in accordance with this Regulation.

9. An exemption decision taken by a Member State pursuant to paragraph 8 shall not prevent an organisation with a principal place of business in the territory of that Member State from deciding to carry out its design and production activities in respect of aircraft covered by that decision in accordance with this Regulation and with the delegated and implementing acts adopted on the basis thereof. Where such an organisation takes such a decision it shall inform the Member State

concerned thereof. In such cases, the exemption decision taken by the Member State pursuant to paragraph 8 shall not apply to those design and production activities or to the aircraft designed and produced as a result of those activities.

10. Without prejudice to obligations of Member States under the Chicago Convention, aircraft to which the exemption decision taken pursuant to paragraph 8 applies and which are registered in the Member State that took that decision may be operated in other Member States, subject to the agreement of the Member State in the territory of which the operation takes place. Such aircraft may also be maintained, or its design may be modified, in other Member States, provided that such maintenance activities and such design modifications are carried out under the oversight of the Member State where the aircraft is registered and in accordance with procedures established in the national law of that Member State.

Any certificate that is issued in respect of aircraft to which an exemption decision taken pursuant to paragraph 8 applies shall clearly indicate that that certificate is issued not under this Regulation but under the national law of the Member State which is issuing the certificate. Other Member States may accept such national certificates only if they themselves have taken a corresponding decision pursuant to paragraph 8.

11. Any provisions of national law of the Member State which has taken an exemption decision pursuant to paragraph 8 regulating the design, production, maintenance and operation activities of the aircraft to which that decision applies shall be proportionate to the nature and risk of the activity concerned and shall take account of the objectives and principles set out in Articles 1 and 4 respectively.

The Member State which has taken an exemption decision pursuant to paragraph 8 shall, without delay, notify the Commission and the Agency of that decision and provide them with all relevant information, and in particular the date from which the that decision applies and the category of aircraft that it concerns.

A Member State may decide to modify or revoke an exemption decision that it has taken pursuant to paragraph 8. In such cases, it shall without delay inform the Commission and the Agency thereof.

The Agency shall include in the repository referred to in Article 74 all of the decisions of the Member States that have been notified pursuant to this paragraph.

An exemption decision taken by a Member State pursuant to paragraph 8 shall also apply to the organisations and personnel involved in the design, production, maintenance and operation activities to which that decision applies.

Article 3. Definitions

For the purposes of this Regulation, the following definitions apply:

(1)‘oversight’ means the verification, by or on behalf of the competent authority, on a continuous basis that the requirements of this Regulation and of the delegated and implementing acts adopted on the basis thereof, on the basis of which a certificate has been issued or in respect of which a declaration has been made, continue to be complied with;

(2)‘Chicago Convention’ means the Convention on International Civil Aviation and the Annexes thereto, signed in Chicago on 7 December 1944;

(3)‘product’ means an aircraft, an engine or a propeller;

(4) ‘part’ means any element of a product, as defined by that product's type design;

(5)‘ATM/ANS’ means air traffic management and air navigation services and covers all of the following: the air traffic management functions and services as defined in point (10) of Article 2 of Regulation (EC) No 549/2004; the air navigation services as defined in point (4) of Article 2 of that Regulation, including the network management functions and services referred to in

Article 6 of Regulation (EC) No 551/2004, as well as services which augment signals emitted by satellites of core constellations of GNSS for the purpose of air navigation; flight procedures design; and services consisting in the origination and processing of data and the formatting and delivering of data to general air traffic for the purpose of air navigation;

(6) 'ATM/ANS constituent' means tangible objects such as hardware and intangible objects such as software upon which the interoperability of the EATMN depends;

(7) 'ATM/ANS system' means the aggregation of airborne and ground-based constituents, as well as space-based equipment, that provides support for air navigation services for all phases of flight;

(8) 'ATM Master Plan' means the plan endorsed by Council Decision 2009/320/EC ([34]), in accordance with Article 1(2) of Council Regulation (EC) No 219/2007 ([35]);

(9) 'certification' means any form of recognition in accordance with this Regulation, based on an appropriate assessment, that a legal or natural person, product, part, non-installed equipment, equipment to control unmanned aircraft remotely, aerodrome, safety-related aerodrome equipment, ATM/ANS system, ATM/ANS constituent or flight simulation training device complies with the applicable requirements of this Regulation and of the delegated and implementing acts adopted on the basis thereof, through the issuance of a certificate attesting such compliance;

(10) 'declaration' means any written statement made in accordance with this Regulation under the sole responsibility of a legal or natural person subject to this Regulation and which confirms that the applicable requirements of this Regulation and of the delegated and implementing acts adopted on the basis thereof relating to a legal or natural person, product, part, non-installed equipment, equipment to control unmanned aircraft remotely, safety-related aerodrome equipment, ATM/ANS system, ATM/ANS constituent or flight simulation training device are complied with;

(11) 'qualified entity' means an accredited legal or natural person which may be charged with certain certification or oversight tasks under this Regulation by and under the control and the responsibility of the Agency or a national competent authority;

(12) 'certificate' means any certificate, approval, licence, authorisation, attestation or other document issued as the result of a certification attesting compliance with the applicable requirements;

(13) 'aircraft operator' means any legal or natural person operating or proposing to operate one or more aircraft;

(14) 'aerodrome operator' means any legal or natural person operating or proposing to operate one or more aerodromes;

(15) 'flight simulation training device' means any type of device in which flight conditions are simulated on the ground, including flight simulators, flight training devices, flight and navigation procedures trainers and basic instrument training devices;

(16) 'aerodrome' means a defined area, on land or on water, on a fixed, fixed offshore or floating structure, including any buildings, installations and equipment thereon, intended to be used either wholly or in part for the arrival, departure and surface movement of aircraft;

(17) 'safety-related aerodrome equipment' means any instrument, equipment, mechanism, apparatus, appurtenance, software or accessory that is used or intended to be used to contribute to the safe operation of aircraft at an aerodrome;

(18) 'apron' means a defined area of an aerodrome intended to accommodate aircraft for purposes of loading or unloading passengers, baggage, mail or cargo, fuelling, parking or maintenance;

(19)‘apron management service (AMS)’ means a service provided to regulate the activities and the movement of aircraft and vehicles on an apron;

(20)‘flight information service’ means a service provided for the purpose of giving advice and information useful for the safe and efficient conduct of flights;

(21)‘general air traffic’ means all movements of civil aircraft and state aircraft carried out in conformity with the procedures of the International Civil Aviation Organization (‘ICAO’);

(22)‘international standards and recommended practices’ means the international standards and recommended practices adopted by ICAO in accordance with Article 37 of the Chicago Convention;

(23)‘groundhandling service’ means any service provided at aerodromes comprising safety - related activities in the areas of ground supervision, flight dispatch and load control, passenger handling, baggage handling, freight and mail handling, apron handling of aircraft, aircraft services, fuel and oil handling, and loading of catering; including the case where aircraft operators provide those groundhandling services to themselves (self-handling);

(24)‘commercial air transport’ means an aircraft operation to transport passengers, cargo or mail for remuneration or other valuable consideration;

(25)‘safety performance’ means the Union's, a Member State's or an organisation's safety achievement, as defined by its safety performance targets and safety performance indicators;

(26)‘safety performance indicator’ means a parameter used for monitoring and assessing safety performance;

(27)‘safety performance target’ means a planned or intended objective for complying with safety performance indicators over a given period of time;

(28)‘aircraft’ means any machine that can derive support in the atmosphere from the reactions of the air other than reactions of the air against the earth's surface;

(29)‘non-installed equipment’ means any instrument, equipment, mechanism, apparatus, appurtenance, software or accessory carried on board of an aircraft by the aircraft operator, which is not a part, and which is used or intended to be used in operating or controlling an aircraft, supports the occupants' survivability, or which could impact the safe operation of the aircraft;

(30)‘unmanned aircraft’ means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board;

(31)‘remote pilot’ means a natural person responsible for safely conducting the flight of an unmanned aircraft by operating its flight controls, either manually or, when the unmanned aircraft flies automatically, by monitoring its course and remaining able to intervene and change the course at any time;

(32)‘equipment to control unmanned aircraft remotely’ means any instrument, equipment, mechanism, apparatus, appurtenance, software or accessory that is necessary for the safe operation of an unmanned aircraft, which is not a part, and which is not carried on board of that unmanned aircraft;

(33)‘Single European Sky airspace’ means airspace above the territory to which the Treaties apply, as well as any other airspace where Member States apply Regulation (EC) No 551/2004 in accordance with Article 1(3) of that Regulation;

(34)‘national competent authority’ means one or more entities designated by a Member State and having the necessary powers and allocated responsibilities for performing the tasks related to certification, oversight and enforcement in accordance with this Regulation and with the

delegated and implementing acts adopted on the basis thereof, and with Regulation (EC) No 549/2004.

Article 4. **Principles for measures under this Regulation**

1. When taking measures under this Regulation the Commission, the Agency and the Member States shall:

(a) reflect the state of the art and best practices in the field of aviation, and take into account worldwide aviation experience and scientific and technical progress in the respective fields;

(b) build on the best available evidence and analysis;

(c) allow for immediate reaction to established causes of accidents, serious incidents and intentional security breaches;

(d) take into account interdependencies between the different domains of aviation safety, and between aviation safety, cyber security and other technical domains of aviation regulation;

(e) lay down, where possible, requirements and procedures in a manner which is performance-based and focuses on objectives to be achieved, while allowing different means of achieving compliance with those performance-based objectives;

(f) promote cooperation and efficient use of resources between authorities at Union and Member State level;

(g) take non-binding measures, including safety promotion actions, where possible;

(h) take into account the international rights and obligations in the field of civil aviation of the Union and of the Member States, including those under the Chicago Convention.

2. The measures taken under this Regulation shall correspond and be proportionate to the nature and risk of each particular activity to which they relate. In preparing and enacting such measures, the Commission, the Agency and the Member States shall take into account, as appropriate for the activity concerned:

(a) whether persons other than flight crew are carried on board, and in particular whether the operation is open to members of the public;

(b) to what extent third parties or property on the ground could be endangered by the activity;

(c) the complexity, performance and operational characteristics of the aircraft involved;

(d) the purpose of the flight, the type of aircraft and type of airspace used;

(e) the type, scale, and complexity of the operation or activity, including, where relevant, the size and type of the traffic handled by the responsible organisation or person;

(f) the extent to which the persons affected by the risks involved in the operation are able to assess and exercise control over those risks;

(g) the results of past certification and oversight activities.

(…)

SECTION VII
Unmanned aircraft

Article 55. Essential requirements for unmanned aircraft

The design, production, maintenance and operation of aircraft referred to in point (a) and (b) of Article 2(1), where it concerns unmanned aircraft, and their engines, propellers, parts, non-installed equipment and equipment to control them remotely, as well as the personnel, including remote pilots, and organisations involved in those activities, shall comply with the essential requirements set out in Annex IX, and, where the delegated acts referred to in Article 58 and the implementing acts referred to in Article 57 so provide, with the essential requirements set out in Annexes II, IV and V.

Article 56. Compliance of unmanned aircraft

1. Taking into account the objectives and the principles set out in Articles 1 and 4, and in particular the nature and risk of the activity concerned, the operational characteristics of the unmanned aircraft concerned and the characteristics of area of operation, a certificate may be required for the design, production, maintenance and operation of unmanned aircraft and their engines, propellers, parts, non-installed equipment and equipment to control them remotely, as well as for the personnel, including remote pilots, and organisations involved in those activities, in accordance with the delegated acts referred to in Article 58 and the implementing acts referred to in Article 57.

2. The certificate referred to in paragraph 1 of this Article shall be issued upon application, when the applicant has demonstrated that it complies with the delegated acts referred to in Article 58 and the implementing acts referred to in Article 57.

3. The certificate referred to in paragraph 1 of this Article shall specify the safety-related limitations, operating conditions and privileges. The certificate may be amended to add or remove limitations, conditions and privileges, in accordance with the delegated acts referred to in Article 58 and the implementing acts referred to in Article 57.

4. The certificate referred to in paragraph 1 of this Article may be limited, suspended or revoked when the holder no longer complies with the conditions, rules and procedures for issuing or maintaining such certificate, in accordance with the delegated acts referred to in Article 58 and the implementing acts referred to in Article 57.

5. Taking into account the objectives and the principles set out in Articles 1 and 4, and in particular the nature and risk of the activity concerned, the operational characteristics of the unmanned aircraft concerned and the characteristics of area of operation, the delegated acts referred to in Article 58 and the implementing acts referred to in Article 57 may require in respect of the design, production, maintenance and operation of unmanned aircraft and their engines, propellers, parts, non-installed equipment and equipment to control them remotely, as well as of the personnel, including remote pilots, and organisations involved in those activities, a declaration confirming compliance with those delegated and implementing acts.

6. Where the objectives and the principles set out in Articles 1 and 4 can be achieved without the application of Chapters IV and V of this Regulation, the delegated acts referred to in point (c) of Article 58(1) might provide that those Chapters shall apply neither to the essential requirements referred to in Article 55 nor to the corresponding detailed rules established in accordance with Article 58. In such cases, those essential requirements and those detailed rules shall constitute 'Community harmonisation legislation' within the meaning of Regulation (EC) No 765/2008 of the European Parliament and of the Council ([36]) and Decision No 768/2008/EC of the European Parliament and of the Council ([37]).

7. Member States shall ensure that information about registration of unmanned aircraft and of operators of unmanned aircraft that are subject to a registration requirement in accordance with

the implementing acts referred to in Article 57 and point 4 of Annex IX is stored in digital, harmonised, interoperable national registration systems. Member States shall be able to access and exchange that information through the repository referred to in Article 74.

8. This Section shall be without prejudice to the possibility for Member States to lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of this Regulation, including public security or protection of privacy and personal data in accordance with the Union law.

Article 57. Implementing acts as regards unmanned aircraft

In order to ensure the uniform implementation of and compliance with the essential requirements referred to in Article 55, for the operation of aircraft referred to in points (a) and (b) of Article 2(1), where it concerns unmanned aircraft, as well as for personnel, including remote pilots, and organisations involved in those activities, and on the basis of the principles set out in Article 4 and with a view to achieving the objectives set out in Article 1, the Commission shall, adopt implementing acts laying down detailed provisions concerning:

(a) the specific rules and procedures for the operation of unmanned aircraft as well as for the personnel, including remote pilots, and organisations involved in those operations;

(b) the rules and procedures for issuing, maintaining, amending, limiting, suspending, or revoking the certificates, or for making declarations, for the operation of unmanned aircraft as well as for personnel, including remote pilots, and organisations involved in those activities, and for the situations in which such certificates or declarations are to be required; the rules and procedures for issuing those certificates and for making those declarations may be based on, or consist of, the detailed requirements referred to in Sections I, II and III;

(c) the privileges and responsibilities of the holders of certificates and of natural and legal persons making declarations;

(d) the rules and procedures for the registration and marking of unmanned aircraft and for the registration of operators of unmanned aircraft, referred to in Section 4 of Annex IX;

(e) the rules and procedures for establishing digital, interoperable, harmonised, national registration systems referred to in Article 56(7);

(f) the rules and procedures for the conversion of national certificates into the certificates required under Article 56(1).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 127(3).

Article 58. Delegated powers

1. For the design, production and maintenance of aircraft referred to in points (a) and (b) of Article 2(1), where it concerns unmanned aircraft, and their engines, propellers, parts, non-installed equipment and equipment to control the aircraft remotely, as well as for the personnel, including remote pilots, and organisations involved in those activities, the Commission is empowered to adopt delegated acts, in accordance with Article 128, laying down detailed rules with regard to:

(a) the specific conditions for the design, production and maintenance of unmanned aircraft and their engines, propellers, parts, non-installed equipment and equipment to control the aircraft remotely, as well as for personnel, including remote pilots, and organisations involved in those activities, necessary to ensure compliance with the essential requirements referred to in Article 55 which may include the conditions under which unmanned aircraft are required to be equipped with necessary features and functionalities related, in particular, to maximum operating distance and altitude limitations, position communication, geographical zones entry restriction, collision avoidance, flight stabilisation and automated landing;

(b) the conditions and procedures for issuing, maintaining, amending, limiting, suspending, or revoking the certificates, or for making declarations, for the design, production and maintenance of unmanned aircraft, their engines, propellers, parts, non-installed equipment and equipment to control them remotely, as well as for the personnel, including remote pilots, and organisations involved in those activities, referred to in Article 56(1) and (5), and for the situations in which such certificates or declarations are to be required; the conditions and procedures for issuing those certificates and for making those declarations may be based on, or consist of, the detailed requirements referred to in Sections I, II and III;

(c) the conditions under which the requirements concerning the design, production and maintenance of unmanned aircraft and their engines, propellers, parts, non-installed equipment and equipment to control them remotely, are not to be subject to Chapters IV and V, for the purpose of Article 56(6);

(d) the privileges and responsibilities of the holders of certificates and of natural and legal persons making declarations;

(e) the conditions for the conversion of national certificates into the certificates required under Article 56(1).

2. As regards the design, production, maintenance and operation of aircraft referred to in points (a) and (b) of Article 2(1), where it concerns unmanned aircraft, and their engines, propellers, parts, non-installed equipment and equipment to control the aircraft remotely, as well as the personnel, including remote pilots, and organisations involved in those activities, the Commission is empowered to adopt delegated acts, in accordance with Article 128, to amend Annex IX and, if applicable, Annex III, where necessary for reasons of technical, operational or scientific developments or safety evidence related to air operations, in order and to the extent required to achieve the objectives set out in Article 1.

(…)

Commission implementing regulation on unmanned aircrafts

Commission implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 216/2008 and (EC) No 552/2004 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [1], and in particular Article 57 thereof,

Whereas:

(1) Unmanned aircraft, irrespective of their mass, can operate within the same Single European Sky airspace, alongside manned aircraft, whether airplanes or helicopters.

(2) As for manned aviation, a uniform implementation of and compliance with rules and procedures should apply to operators, including remote pilots, of unmanned aircraft and unmanned aircraft system ('UAS'), as well as for the operations of such unmanned aircraft and unmanned aircraft system.

(3) Considering the specific characteristics of UAS operations, they should be as safe as those in manned aviation.

(4) Technologies for unmanned aircraft allow a wide range of possible operations. Requirements related to the airworthiness, the organisations, the persons involved in the operation of UAS and unmanned aircraft operations should be set out in order to ensure safety for people on the ground and other airspace users during the operations of unmanned aircraft.

(5) The rules and procedures applicable to UAS operations should be proportionate to the nature and risk of the operation or activity and adapted to the operational characteristics of the unmanned aircraft concerned and the characteristics of the area of operations, such as the population density, surface characteristics, and the presence of buildings.

(6) The risk level criteria as well as other criteria should be used to establish three categories of operations: the 'open', 'specific' and 'certified' categories.

(7) Proportionate risks mitigation requirements should be applicable to UAS operations according to the level of risk involved, the operational characteristics of the unmanned aircraft concerned and the characteristics of the area of operation.

(8) Operations in the 'open' category, which should cover operations that present the lowest risks, should not require UAS that are subject to standard aeronautical compliance procedures, but should be conducted using the UAS classes that are defined in Commission Delegated Regulation (EU) 2019/945 [2].

(9) Operations in the 'specific' category should cover other types of operations presenting a higher risk and for which a thorough risk assessment should be conducted to indicate which requirements are necessary to keep the operation safe.

(10) A system of declaration by an operator should facilitate the enforcement of this Regulation in case of low risk operations conducted in the 'specific' category for which a standard scenario has been defined with detailed mitigation measures.

(11) Operations in the 'certified' category should, as a principle, be subject to rules on certification of the operator, and the licensing of remote pilots, in addition to the certification of the aircraft pursuant to Delegated Regulation (EU) 2019/945.

(12) Whilst mandatory for the 'certified category', for the 'specific' category a certificate delivered by the competent authorities for the operation of an unmanned aircraft, as well as for the personnel, including remote pilots and organisations involved in those activities, or for the aircraft pursuant to Delegated Regulation (EU) 2019/945 could also be required.

(13) Rules and procedures should be established for the marking and identification of unmanned aircraft and for the registration of operators of unmanned aircraft or certified unmanned aircraft.

(14) Operators of unmanned aircraft should be registered where they operate an unmanned aircraft which, in case of impact, can transfer, to a human, a kinetic energy above 80 Joules or the operation of which presents risks to privacy, protection of personal data, security or the environment.

(15) Studies have demonstrated that unmanned aircraft with a take-off mass of 250 g or more would present risks to security and therefore UAS operators of such unmanned aircraft should be required to register themselves when operating such aircraft in the 'open' category.

(16) Considering the risks to privacy and protection of personal data, operators of unmanned aircraft should be registered if they operate an unmanned aircraft which is equipped with a sensor able to capture personal data. However, this should not be the case when the unmanned aircraft is considered to be a toy within the meaning of Directive 2009/48/EC of the European Parliament and of the Council on the safety of toys [3].

(17) The information about registration of certified unmanned aircraft and of operators of unmanned aircraft that are subject to a registration requirement should be stored in digital, harmonised, interoperable national registration systems, allowing competent authorities to access and exchange that information. The mechanisms to ensure the interoperability of the national registers in this Regulation should be without prejudice to the rules applicable to the future repository referred to in Article 74 of Regulation (EU) 2018/1139.

(18) In accordance with paragraph 8 of Article 56 of Regulation (EU) 2018/1139, this Regulation is without prejudice to the possibility for Member States to lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of Regulation (EU) 2018/1139, including public security or protection of privacy and personal data in accordance with the Union law.

(19) National registration systems should comply with the applicable Union and national law on privacy and processing of personal data and the information stored in those registrations systems should be easily accessible [4].

(20) UAS operators and remote pilots should ensure that they are adequately informed about applicable Union and national rules relating to the intended operations, in particular with regard to safety, privacy, data protection, liability, insurance, security and environmental protection.

(21) Some areas, such as hospitals, gatherings of people, installations and facilities like penal institutions or industrial plants, top-level and higher-level government authorities, nature conservation areas or certain items of transport infrastructure, can be particularly sensitive to some or all types of UAS operations. This should be without prejudice to the possibility for

Member States to lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of this Regulation, including environmental protection, public security or protection of privacy and personal data in accordance with the Union law.

(22) Unmanned aircraft noise and emissions should be minimised as far as possible taking into account the operating conditions and various specific characteristics of individual Member States, such as the population density, where noise and emissions are of concern. In order to facilitate the societal acceptance of UAS operations, Delegated Regulation (EU) 2019/945 includes maximum level of noise for unmanned aircraft operated close to people in the 'open' category. In the 'specific' category there is a requirement for the operator to develop guidelines for its remote pilots so that all operations are flown in a manner that minimises nuisances to people and animals.

(23) Current national certificates should be adapted to certificates complying with the requirements of this Regulation.

(24) In order to ensure the proper implementation of this Regulation, appropriate transitional measures should be established. In particular, Member States and stakeholders should have sufficient time to adapt their procedures to the new regulatory framework before this Regulation applies.

(25) The new regulatory framework for UAS operations should be without prejudice to the applicable environmental and nature protection obligations otherwise stemming from national or Union law.

(26) While the 'U-space' system including the infrastructure, services and procedures to guarantee safe UAS operations and supporting their integration into the aviation system is in development, this Regulation should already include requirements for the implementation of three foundations of the U-space system, namely registration, geo-awareness and remote identification, which will need to be further completed.

(27) Since model aircraft are considered as UAS and given the good safety level demonstrated by model aircraft operations in clubs and associations, there should be a seamless transition from the different national systems to the new Union regulatory framework, so that model aircraft clubs and associations can continue to operate as they do today, as well as taking into account existing best practices in the Member States.

(28) In addition, considering the good level of safety achieved by aircraft of class C4 as provided in Annex to this Regulation, low risk operations of such aircraft should be allowed to be conducted in the 'open' category. Such aircraft, often used by model aircraft operators, are comparatively simpler than other classes of unmanned aircraft and should therefore not be subject to disproportionate technical requirements.

(29) The measures provided for in this Regulation are in accordance with the opinion of the committee established in accordance with Article 127 of Regulation (EU) 2018/1139,

HAS ADOPTED THIS REGULATION:

Article 1. **Subject matter**
This Regulation lays down detailed provisions for the operation of unmanned aircraft systems as well as for personnel, including remote pilots and organisations involved in those operations.

Article 2. Definitions
For the purposes of this Regulation, the definitions in Regulation (EU) 2018/1139 apply.

The following definitions also apply:

The following definitions also apply:

(1) 'unmanned aircraft system' ('UAS') means an unmanned aircraft and the equipment to control it remotely;

(2) 'unmanned aircraft system operator' ('UAS operator') means any legal or natural person operating or intending to operate one or more UAS;

(3) 'assemblies of people' means gatherings where persons are unable to move away due to the density of the people present;

(4) 'UAS geographical zone' means a portion of airspace established by the competent authority that facilitates, restricts or excludes UAS operations in order to address risks pertaining to safety, privacy, protection of personal data, security or the environment, arising from UAS operations;

(5) 'robustness' means the property of mitigation measures resulting from combining the safety gain provided by the mitigation measures and the level of assurance and integrity that the safety gain has been achieved;

(6) 'standard scenario' means a type of UAS operation in the 'specific' category, as defined in Appendix 1 of the Annex, for which a precise list of mitigating measures has been identified in such a way that the competent authority can be satisfied with declarations in which operators declare that they will apply the mitigating measures when executing this type of operation;

(7) 'visual line of sight operation' ('VLOS') means a type of UAS operation in which, the remote pilot is able to maintain continuous unaided visual contact with the unmanned aircraft, allowing the remote pilot to control the flight path of the unmanned aircraft in relation to other aircraft, people and obstacles for the purpose of avoiding collisions;

(8) 'beyond visual line of sight operation' ('BVLOS') means a type of UAS operation which is not conducted in VLOS;

(9) 'light UAS operator certificate' ('LUC') means a certificate issued to a UAS operator by a competent authority as set out in part C of the Annex;

(10) 'model aircraft club or association' means an organisation legally established in a Member State for the purpose of conducting leisure flights, air displays, sporting activities or competition activities using UAS;

(11) 'dangerous goods' means articles or substances, which are capable of posing a hazard to health, safety, property or the environment in the case of an incident or accident, that the unmanned aircraft is carrying as its payload, including in particular:

(a) explosives (mass explosion hazard, blast projection hazard, minor blast hazard, major fire hazard, blasting agents, extremely insensitive explosives);

(b) gases (flammable gas, non-flammable gas, poisonous gas, oxygen, inhalation hazard);

(c) flammable liquids (flammable liquids; combustible, fuel oil, gasoline);

(d) flammable solids (flammable solids, spontaneously combustible solids, dangerous when wet);

(e) oxidising agents and organic peroxides;

(f) toxic and infectious substances (poison, biohazard);

(g) radioactive substances;

(h) corrosive substances;

(12)'payload' means instrument, mechanism, equipment, part, apparatus, appurtenance, or accessory, including communications equipment, that is installed in or attached to the aircraft and is not used or intended to be used in operating or controlling an aircraft in flight, and is not part of an airframe, engine, or propeller;

(13)'direct remote identification' means a system that ensures the local broadcast of information about a unmanned aircraft in operation, including the marking of the unmanned aircraft, so that this information can be obtained without physical access to the unmanned aircraft;

(14)'follow-me mode' means a mode of operation of a UAS where the unmanned aircraft constantly follows the remote pilot within a predetermined radius;

(15)'geo-awareness' means a function that, based on the data provided by Member States, detects a potential breach of airspace limitations and alerts the remote pilots so that they can take immediate and effective action to prevent that breach;

(16)'privately built UAS' means a UAS assembled or manufactured for the builder's own use, not including UAS assembled from sets of parts placed on the market as a single ready-to-assemble kit;

(17)'autonomous operation' means an operation during which an unmanned aircraft operates without the remote pilot being able to intervene;

(18)'uninvolved persons' means persons who are not participating in the UAS operation or who are not aware of the instructions and safety precautions given by the UAS operator;

(19)'making available on the market' means any supply of a product for distribution, consumption or use on the Union market in the course of a commercial activity, whether in exchange of payment or free of charge;

(20)'placing on the market' means the first making available of a product on the Union market;

(21)'controlled ground area' means the ground area where the UAS is operated and within which the UAS operator can ensure that only involved persons are present;

(22)'maximum take-off mass' ('MTOM') means the maximum Unmanned Aircraft mass, including payload and fuel, as defined by the manufacturer or the builder, at which the Unmanned Aircraft can be operated;

(23)'unmanned sailplane' means an unmanned aircraft that is supported in flight by the dynamic reaction of the air against its fixed lifting surfaces, the free flight of which does not depend on an engine. It may be equipped with an engine to be used in case of emergency.

Article 3. **Categories of UAS operations**

UAS operations shall be performed in the 'open', 'specific' or 'certified' category defined respectively in Articles 4, 5 and 6, subject to the following conditions:

(a)UAS operations in the 'open' category shall not be subject to any prior operational authorisation, nor to an operational declaration by the UAS operator before the operation takes place;

(b)UAS operations in the 'specific' category shall require an operational authorisation issued by the competent authority pursuant to Article 12 or an authorisation received in accordance with Article 16, or, under circumstances defined in Article 5(5), a declaration to be made by a UAS operator;

(c) UAS operations in the 'certified' category shall require the certification of the UAS pursuant to Delegated Regulation (EU) 2019/945 and the certification of the operator and, where applicable, the licensing of the remote pilot.

Article 4. **'Open' category of UAS operations**

1. Operations shall be classified as UAS operations in the 'open' category only where the following requirements are met:

(a) the UAS belongs to one of the classes set out in Delegated Regulation (EU) 2019/945 or is privately built or meets the conditions defined in Article 20;

(b) the unmanned aircraft has a maximum take-off mass of less than 25 kg;

(c) the remote pilot ensures that the unmanned aircraft is kept at a safe distance from people and that it is not flown over assemblies of people;

(d) the remote pilot keeps the unmanned aircraft in VLOS at all times except when flying in follow-me mode or when using an unmanned aircraft observer as specified in Part A of the Annex;

(e) during flight, the unmanned aircraft is maintained within 120 metres from the closest point of the surface of the earth, except when overflying an obstacle, as specified in Part A of the Annex

(f) during flight, the unmanned aircraft does not carry dangerous goods and does not drop any material;

2. UAS operations in the 'open' category shall be divided in three sub-categories in accordance with the requirements set out in Part A of the Annex.

Article 5. **'Specific' category of UAS operations**

1. Where one of the requirements laid down in Article 4 or in Part A of the Annex is not met, a UAS operator shall be required to obtain an operational authorisation pursuant to Article 12 from the competent authority in the Member State where it is registered.

2. When applying to a competent authority for an operational authorisation pursuant Article 12, the operator shall perform a risk assessment in accordance with Article 11 and submit it together with the application, including adequate mitigating measures.

3. In accordance with point UAS.SPEC.040 laid down in Part B of the Annex, the competent authority shall issue an operational authorisation, if it considers that the operational risks are adequately mitigated in accordance with Article 12.

4. The competent authority shall specify whether the operational authorisation concerns:

(a) the approval of a single operation or a number of operations specified in time or location(s) or both. The operational authorisation shall include the associated precise list of mitigating measures;

(b) the approval of an LUC, in accordance with part C of the Annex.

5. Where the UAS operator submits a declaration to the competent authority of the Member State of registration in accordance with point UAS.SPEC.020 laid down in Part B of the Annex for an operation complying with a standard scenario as defined in Appendix 1 to that Annex, the UAS operator shall not be required to obtain an operational authorisation in accordance with paragraphs 1 to 4 of this Article and the procedure laid down in paragraph 5 of Article 12 shall apply.

6. An operational authorisation or a declaration shall not be required for:

(a)UAS operators holding an LUC with appropriate privileges in accordance with point UAS.LUC.060 of the Annex;

(b)operations conducted in the framework of model aircraft clubs and associations that have received an authorisation in accordance with Article 16.

Article 6. **'Certified' category of UAS operations**

1. Operations shall be classified as UAS operations in the 'certified' category only where the following requirements are met:

(a)the UAS is certified pursuant to points (a), (b) and (c) of paragraph 1 of Article 40 of Delegated Regulation (EU) 2019/945; and

(b)the operation is conducted in any of the following conditions:

i. over assemblies of people;

ii. involves the transport of people;

iii.involves the carriage of dangerous goods, that may result in high risk for third parties in case of accident.

2. In addition, UAS operations shall be classified as UAS operations in the 'certified' category where the competent authority, based on the risk assessment provided for in Article 11, considers that the risk of the operation cannot be adequately mitigated without the certification of the UAS and of the UAS operator and, where applicable, without the licensing of the remote pilot.

Article 7. **Rules and procedures for the operation of UAS**

1. UAS operations in the 'open' category shall comply with the operational limitations set out in Part A of the Annex.

2. UAS operations in the 'specific' category shall comply with the operational limitations set out in the operational authorisation as referred to in Article 12 or the authorisation as referred to in Article 16, or in a standard scenario defined in Appendix 1 to the Annex as declared by the UAS operator.

This paragraph shall not apply where the UAS operator holds an LUC with appropriate privileges.

UAS operations in the 'specific' category shall be subject to the applicable operational requirements laid down in Commission Implementing Regulation (EU) No 923/2012 ([5]).

3. UAS operations in the 'certified' category shall be subject to the applicable operational requirements laid down in Implementing Regulation (EU) No 923/2012 and Commission Regulations (EU) No 965/2012 [6] and (EU) No 1332/2011 [7].

Article 8. **Rules and procedures for the competency of remote pilots**

1. Remote pilots operating UAS in the 'open' category shall comply with the competency requirements set in Part A of the Annex.

2. Remote pilots operating UAS in the 'specific' category shall comply with the competency requirements set out in the operational authorisation by the competent authority or in the standard scenario defined in Appendix 1 to the Annex or as defined by the LUC and shall have at least the following competencies:

(a)ability to apply operational procedures (normal, contingency and emergency procedures, flight planning, pre-flight and post-flight inspections);

(b)ability to manage aeronautical communication;

(c) manage the unmanned aircraft flight path and automation;

(d) leadership, teamwork and self-management;

(e) problem solving and decision-making;

(f) situational awareness;

(g) workload management;

(h) coordination or handover, as applicable.

3. Remote pilots operating in the framework of model aircraft clubs or associations shall comply with the minimum competency requirements defined in the authorisation granted in accordance with Article 16.

Article 9. **Minimum age for remote pilots**

1. The minimum age for remote pilots operating a UAS in the 'open' and 'specific' category shall be 16 years.

2. No minimum age for remote pilots shall be required:

(a) when they operate in subcategory A1 as specified in Part A of the Annex to this Regulation, with a UAS Class C0 defined in Part 1 of the Annex to Delegated Regulation (EU) 2019/945 that is a toy within the meaning of Directive 2009/48/EC;

(b) for privately-built UAS with a maximum take-off mass of less than 250g;

(c) when they operate under the direct supervision of a remote pilot complying with paragraph 1 and Article 8.

3. Member States may lower the minimum age following a risk-based approach taking into account specific risks associated with the operations in their territory:

(a) for remote pilots operating in the 'open' category by up to 4 years;

(b) for remote pilots operating in the 'specific' category by up to 2 years.

4. Where a Member State lowers the minimum age for remote pilots, those remote pilots shall only be allowed to operate a UAS on the territory of that Member State.

5. Member States may define a different minimum age for remote pilots operating in the framework of model aircraft clubs or associations in the authorisation issued in accordance with Article 16.

Article 10. **Rules and procedures for the airworthiness of UAS**

Unless privately-built, or used for operations referred to in Article 16, or meeting the conditions defined in Article 20, UAS used in operations set out in this Regulation shall comply with the technical requirements and rules and procedures for the airworthiness defined in the delegated acts adopted pursuant to Article 58 of Regulation (EU) 2018/1139.

Article 11. **Rules for conducting an operational risk assessment**

1. An operational risk assessment shall:

(a) describe the characteristics of the UAS operation;

(b) propose adequate operational safety objectives;

(c) identify the risks of the operation on the ground and in the air considering all of the below:

i. the extent to which third parties or property on the ground could be endangered by the activity;

ii.the complexity, performance and operational characteristics of the unmanned aircraft involved;

iii.the purpose of the flight, the type of UAS, the probability of collision with other aircraft and class of airspace used;

iv.the type, scale, and complexity of the UAS operation or activity, including, where relevant, the size and type of the traffic handled by the responsible organisation or person;

v.the extent to which the persons affected by the risks involved in the UAS operation are able to assess and exercise control over those risks.

(d)identify a range of possible risk mitigating measures;

(e)determine the necessary level of robustness of the selected mitigating measures in such a way that the operation can be conducted safely.

2. The description of the UAS operation shall include at least the following:

(a)the nature of the activities performed;

(b)the operational environment and geographical area for the intended operation, in particular overflown population, orography, types of airspace, airspace volume where the operation will take place and which airspace volume is kept as necessary risk buffers, including the operational requirements for geographical zones;

(c)the complexity of the operation, in particular which planning and execution, personnel competencies, experience and composition, required technical means are planned to conduct the operation;

(d)the technical features of the UAS, including its performance in view of the conditions of the planned operation and, where applicable, its registration number;

(e)the competence of the personnel for conducting the operation including their composition, role, responsibilities, training and recent experience.

3. The assessment shall propose a target level of safety, which shall be equivalent to the safety level in manned aviation, in view of the specific characteristics of UAS operation.

4. The identification of the risks shall include the determination of all of the below:

(a)the unmitigated ground risk of the operation taking into account the type of operation and the conditions under which the operation takes place, including at least the following criteria:

i. VLOS or BVLOS;

ii. population density of the overflown areas;

iii. flying over an assembly of people;

iv. the dimension characteristics of the unmanned aircraft;

(b)the unmitigated air risk of the operation taking into account all of the below:

i. the exact airspace volume where the operation will take place, extended by a volume of airspace necessary for contingency procedures;

ii. the class of the airspace;

iii. the impact on other air traffic and air traffic management (ATM) and in particular:

— the altitude of the operation;

— controlled versus uncontrolled airspace;

— aerodrome versus non-aerodrome environment;

— airspace over urban versus rural environment;

— separation from other traffic.

5. The identification of the possible mitigation measures necessary to meet the proposed target level of safety shall consider the following possibilities:

(a) containment measures for people on the ground;

(b) strategic operational limitations to the UAS operation, in particular:

i. restricting the geographical volumes where the operation takes place;

ii. restricting the duration or schedule of the time slot in which the operation takes place;

(c) strategic mitigation by common flight rules or common airspace structure and services;

(d) capability to cope with possible adverse operating conditions;

(e) organisation factors such as operational and maintenance procedures elaborated by the UAS operator and maintenance procedures compliant with the manufacturer's user manual;

(f) the level of competency and expertise of the personnel involved in the safety of the flight;

(g) the risk of human error in the application of the operational procedures;

(h) the design features and performance of the UAS in particular:

i. the availability of means to mitigate risks of collision;

ii. the availability of systems limiting the energy at impact or the frangibility of the unmanned aircraft;

iii. the design of the UAS to recognised standards and the fail-safe design.

6. The robustness of the proposed mitigating measures shall be assessed in order to determine whether they are commensurate with the safety objectives and risks of the intended operation, particularly to make sure that every stage of the operation is safe.

Article 12. Authorising operations in the 'specific' category

1. The competent authority shall evaluate the risk assessment and the robustness of the mitigating measures that the UAS operator proposes to keep the UAS operation safe in all phases of flight.

2. The competent authority shall grant an operational authorisation when the evaluation concludes that:

(a) the operational safety objectives take account of the risks of the operation;

(b) the combination of mitigation measures concerning the operational conditions to perform the operations, the competence of the personnel involved and the technical features of the unmanned aircraft, are adequate and sufficiently robust to keep the operation safe in view of the identified ground and air risks;

(c) the UAS operator has provided a statement confirming that the intended operation complies with any applicable Union and national rules relating to it, in particular, with regard to privacy, data protection, liability, insurance, security and environmental protection.

3. When the operation is not deemed sufficiently safe, the competent authority shall inform the applicant accordingly, giving reasons for its refusal to issue the operational authorisation.

4. The operational authorisation granted by the competent authority shall detail:

(a) the scope of the authorisation;

(b) the 'specific' conditions that shall apply:

i. to the UAS operation and the operational limitations;

ii. to the required competency of the UAS operator and, where applicable, of the remote pilots;

iii. to the technical features of the UAS, including the certification of the UAS, if applicable;

(c) the following information:

i. the registration number of the UAS operator and the technical features of the UAS;

ii. a reference to the operational risk assessment developed by the UAS operator;

iii. the operational limitations and conditions of the operation;

iv. the mitigation measures that the UAS operator has to apply;

v. the location(s) where the operation is authorised to take place and any other locations in a Member States in accordance with Article 13;

vi. all documents and records relevant for the type of operation and the type of events that should be reported in addition to those defined in Regulation (EU) No 376/2014 of the European Parliament and of the Council [8].

5. Upon receipt of the declaration referred to in paragraph 5 of Article 5, the competent authority shall:

(a) verify that it contains all elements set out in paragraph 2 of point UAS.SPEC.020 of the Annex;

(b) if this is the case, provide the UAS operator with a confirmation of receipt and completeness without undue delay so that the operator may start the operation.

Article 13. Cross-border operations or operations outside the state of registration

1. When an UAS operator intends to conduct an operation in the 'specific' category for which an operational authorisation has already been granted in accordance with Article 12, and which is intended to take place partially or entirely in the airspace of a Member State other than the Member State of registration, the UAS operator shall provide the competent authority of the Member State of intended operation with an application including the following information:

(a) a copy of the operational authorisation granted to the UAS operator in accordance with Article 12; and

(b) the location(s) of the intended operation including the updated mitigation measures, if needed, to address those risks identified under Article 11(2)(b) which are specific to the local airspace, terrain and population characteristics and the climatic conditions.

2. Upon receipt of the application set out in paragraph 1, the competent authority of the Member State of intended operation shall assess it without undue delay and provide the competent authority of the Member State of registration and the UAS operator with a confirmation that the updated mitigation measures referred to in point (b) of paragraph 1 are satisfactory for the operation at the intended location. Upon receipt of that confirmation, the UAS operator may start the intended operation and the Member State of registration shall record the updated mitigation measures that the UAS operator has to apply in the operational authorisation issued in accordance with Article 12.

3. When an UAS operator intends to conduct an operation in the 'specific' category for which a declaration has been made in accordance with paragraph 5 of Article 5, and which is intended to take place partially or entirely in the airspace of a Member State other than the Member State of registration, the UAS operator shall provide the competent authority of the Member State of the intended operation with a copy of the declaration submitted to the Member State of registration, as well as a copy of the confirmation of receipt and completeness.

Article 14. **Registration of UAS operators and certified UAS**

1. Member States shall establish and maintain accurate registration systems for UAS whose design is subject to certification and for UAS operators whose operation may present a risk to safety, security, privacy, and protection of personal data or environment.

2. The registration systems for UAS operators shall provide the fields for introducing and exchanging the following information:

(a) the full name and the date of birth for natural persons and the name and their identification number for legal persons;

(b) the address of UAS operators;

(c) their email address and telephone number;

(d) an insurance policy number for UAS if required by Union or national law;

(e) the confirmation by legal persons of the following statement: 'All personnel directly involved in the operations are competent to perform their tasks, and the UAS will be operated only by remote pilots with the appropriate level of competency';

(f) operational authorisations and LUCs held and declarations followed by a confirmation in accordance with Article 12(5)(b).

3. The registration systems for unmanned aircraft whose design is subject to certification shall provide the fields for introducing and exchanging the following information:

(a) manufacturer's name;

(b) manufacturer's designation of the unmanned aircraft;

(c) unmanned aircraft's serial number;

(d) full name, address, email address and telephone number of the natural or legal person under whose name the unmanned aircraft is registered.

4. Member States shall ensure that registration systems are digital and interoperable and allow for mutual access and exchange of information through the repository referred to in Article 74 of Regulation (EU) 2018/1139.

5. UAS operators shall register themselves:

(a) when operating within the 'open' category any of the following unmanned aircraft:

i. with a MTOM of 250 g or more, or, which in the case of an impact can transfer to a human kinetic energy above 80 Joules;

ii. that is equipped with a sensor able to capture personal data, unless it complies with Directive 2009/48/EC.

(b) when operating within the 'specific' category an unmanned aircraft of any mass.

6. UAS operators shall register themselves in the Member State where they have their residence for natural persons or where they have their principal place of business for legal persons and ensure that their registration information is accurate. A UAS operator cannot be registered in more than one Member State at a time.

Member States shall issue a unique digital registration number for UAS operators and for the UAS that require registration, allowing their individual identification.

The registration number for UAS operators shall be established on the basis of standards that support the interoperability of the registration systems;

7. The owner of an unmanned aircraft whose design is subject to certification shall register the unmanned aircraft.

The nationality and registration mark of an unmanned aircraft shall be established in line with ICAO Annex 7. An unmanned aircraft cannot be registered in more than one State at a time.

8. The UAS operators shall display their registration number on every unmanned aircraft meeting the conditions described in paragraph 5.

Article 15. Operational conditions for UAS geographical zones

1. When defining UAS geographical zones for safety, security, privacy or environmental reasons, Member States may:

(a) prohibit certain or all UAS operations, request particular conditions for certain or all UAS operations or request a prior operational authorisation for certain or all UAS operations;

(b) subject UAS operations to specified environmental standards;

(c) allow access to certain UAS classes only;

(d) allow access only to UAS equipped with certain technical features, in particular remote identification systems or geo awareness systems.

2. On the basis of a risk assessment carried out by the competent authority, Member States may designate certain geographical zones in which UAS operations are exempt from one or more of the 'open' category requirements.

3. When pursuant to paragraphs 1 or 2 Member States define UAS geographical zones, for geo awareness purposes they shall ensure that the information on the UAS geographical zones, including their period of validity, is made publicly available in a common unique digital format.

Article 16. UAS operations in the framework of model aircraft clubs and associations

1. Upon request by a model aircraft club or association, the competent authority may issue an authorisation for UAS operations in the framework of model aircraft clubs and associations.

2. The authorisation referred to in paragraph 1 shall be issued in accordance with any of the following:

(a) relevant national rules;

(b) established procedures, organisational structure and management system of the model aircraft club or association, ensuring that:

i. remote pilots operating in the framework of model aircraft clubs or associations are informed of the conditions and limitations defined in the authorisation issued by the competent authority;

ii. remote pilots operating in the framework of model aircraft clubs or associations are assisted in achieving the minimum competency required to operate the UAS safely and in accordance with the conditions and limitations defined in the authorisation;

iii. the model aircraft club or association takes appropriate action when informed that a remote pilot operating in the framework of model aircraft clubs or associations does not comply with the conditions and limitations defined in the authorisation, and, if necessary, inform the competent authority;

iv. the model aircraft club or association provides, upon request from the competent authority, documentation required for oversight and monitoring purposes.

3. The authorisation referred to in paragraph 1 shall specify the conditions under which operations in the framework of the model aircraft clubs or associations may be conducted and shall be limited to the territory of the Member State in which it is issued.

4. Member States may enable model aircraft clubs and associations to register their members into the registration systems established in accordance with Article 14 on their behalf. If this is not the case, the members of model aircraft clubs and associations shall register themselves in accordance with Article 14.

Article 17. Designation of the competent authority

1. Each Member State shall designate one or more entities as the competent authority for the tasks referred to in Article 18.

2. Where a Member State designates more than one entity as a competent authority it shall:

(a) clearly define the areas of competence of each competent authority in terms of responsibilities;

(b) establish appropriate coordination mechanism between those entities to ensure the effective oversight of all organisations and persons subject to this Regulation.

Article 18. Tasks of the competent authority

The competent authority shall be responsible for:

(a) enforcing this Regulation;

(b) issuing, suspending or revoking certificates of UAS operators and licenses of remote pilots operating within the 'certified' category of UAS operations;

(c) issuing remote pilots with a proof of completion of an online theoretical knowledge examination according to points UAS.OPEN.020 and UAS.OPEN.040 of the Annex and issuing, amending, suspending, limiting or revoking certificates of competency of remote pilots according to point UAS.OPEN.030 of the Annex;

(d) issuing, amending, suspending, limiting or revoking operational authorisations and LUCs and verifying completeness of declarations, which are required to carry out UAS operations in the 'specific' category of UAS operations;

(e) keeping documents, records and reports concerning UAS operational authorisations, declarations, certificates of competency of the remote pilots and LUCs;

(f) making available in a common unique digital format information on UAS geographical zones identified by the Member States and established within the national airspace of its State;

(g) issuing a confirmation of receipt and completeness in accordance with Article 12(5)(b) or a confirmation in accordance with paragraph 2 of Article 13;

(h) developing a risk-based oversight system for:

  i. UAS operators that have submitted a declaration or hold an operational authorisation or an LUC;

  ii. model clubs and associations that hold an authorisation referred to in Article 16;

(i) for operations other than those in the 'open' category, establishing audit planning based on the risk profile, compliance level and the safety performance of UAS operators who have submitted a declaration, or hold a certificate issued by the competent authority;

(j) for operations other than those in the 'open' category, carrying out inspections with regard to UAS operators who have submitted a declaration or hold a certificate issued by the competent authority inspecting UAS and ensuring that UAS operators and remote pilots comply with this Regulation;

(k) implementing a system to detect and examine incidents of non-compliance by UAS operators operating in the 'open' or 'specific' categories and reported in accordance with paragraph 2 of Article 19;

(l) providing UAS operators with information and guidance that promotes the safety of UAS operations;

(m) establishing and maintaining registration systems for UAS whose design is subject to certification and for UAS operators whose operation may present a risk to safety, security, privacy, and protection of personal data or the environment.

Article 19. **Safety information**

1. The competent authorities of the Member States and market surveillance and control authorities referred to in Article 36 of Delegated Regulation (EU) 2019/945 shall cooperate on safety matters and establish procedures for the efficient exchange of safety information.

2. Each UAS operator shall report to the competent authority on any safety-related occurrence and exchange information regarding its UAS in compliance with Regulation (EU) No 376/2014.

3. The European Union Aviation Safety Agency ('the Agency') and the competent authorities shall collect, analyse and publish safety information concerning UAS operations in their territory in accordance with Article 119 of Regulation (EU) 2018/1139 and its implementing acts.

4. Upon receiving any of the information referred to in paragraphs 1, 2 or 3, the Agency and the competent authority shall take the necessary measures to address any safety issues on the best available evidence and analysis, taking into account interdependencies between the different domains of aviation safety, and between aviation safety, cyber security and other technical domains of aviation regulation.

5. Where the competent authority or the Agency takes measures in accordance with paragraph 4, it shall immediately notify all relevant interested parties and organisations that need to comply with those measures in accordance with Regulation (EU) 2018/1139 and its implementing acts.

Article 20. **Particular provisions concerning the use of certain UAS in the 'open' category**

UAS types within the meaning of Decision No 768/2008/EC of the European Parliament and of the Council [9], which do not comply with Delegated Regulation (EU) 2019/945 and which are not privately-built are allowed to continue to be operated under the following conditions, when they have been placed on the market before 1 July 2022:

(a) in subcategory A1 as defined in Part A of the Annex, provided that the unmanned aircraft has a maximum take-off mass of less than 250 g, including its payload;

(b) in subcategory A3 as defined in Part A of the Annex, provided that the unmanned aircraft has a maximum take-off mass of less than 25 kg, including its fuel and payload.

Article 21. **Adaptation of authorisations, declarations and certificates**

1. Authorisations granted to UAS operators, certificates of remote pilot competency and declarations made by UAS operators or equivalent documentation, issued on the basis of national law, shall remain valid until 1 July 2021.

2. By 1 July 2021 Member States shall convert their existing certificates of remote pilot competency and their UAS operator authorisations or declarations, or equivalent documentation, including those issued until that date, in accordance with this Regulation.

3. Without prejudice to Article 14, UAS operations conducted in the framework of model aircraft clubs and associations shall be allowed to continue in accordance with relevant national rules and without an authorisation in accordance with Article 16 until 1 July 2022.

Article 22. Transitional provisions

Without prejudice to Article 20, the use of UAS in the 'open' category which do not comply with the requirements of Parts 1 to 5 of the Annex to Delegated Regulation (EU) 2019/945 shall be allowed for a transitional period of two years starting one year after the date of entry into force of this Regulation, subject to the following conditions:

(a) unmanned aircraft with a maximum take-off mass of less than 500 g are operated within the operational requirements set out in points UAS.OPEN.020(1) of Part A of the Annex by a remote pilot having competency level defined by the Member State concerned;

(b) unmanned aircraft with a maximum take-off mass of less than 2 kg is operated by keeping a minimum horizontal distance of 50 meters from people and the remote pilots have a competency level at least equivalent to the one set out in point UAS.OPEN.030(2) of Part A of the Annex;

(c) unmanned aircraft with a maximum take-off mass of more than 2 kg and less than 25kg is operated within the operational requirements set out in point UAS.OPEN.040(1) and (2) and the remote pilots have a competency level at least equivalent to the one set out in point UAS.OPEN.020(4)(b) of Part A of the Annex.

Article 23. Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 1 July 2020.

2. Paragraph 5 of Article 5 shall apply as from the date on which Appendix 1 of the Annex is amended so that it contains the applicable standard scenarios. Member States may in accordance with paragraph 5 of Article 5 accept declarations by UAS operators based on national standard scenarios, if those scenarios meet the requirements of point UAS.SPEC.020 of the Annex until this Regulation is amended to include the standard scenario in Appendix 1 of the Annex.

3. Paragraph 3 of Article 15 shall apply from 1 July 2021.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 24 May 2019.

For the Commission

The President

Jean-Claude JUNCKER

([1]) OJ L 212, 22.8.2018, p. 1.

([2]) Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (see page 1 of this Official Journal).

([3]) Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1).

([4]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([5]) Commission Implementing Regulation (EU) No 923/2012 of 26 September 2012 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation and amending Implementing Regulation (EU) No 1035/2011 and Regulations (EC) No 1265/2007, (EC) No 1794/2006, (EC) No 730/2006, (EC) No 1033/2006 and (EU) No 255/2010 (OJ L 281, 13.10.2012, p. 1).

([6]) Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 296, 25.10.2012, p. 1).

([7]) Commission Regulation (EU) No 1332/2011 of 16 December 2011 laying down common airspace usage requirements and operating procedures for airborne collision avoidance (OJ L 336, 20.12.2011, p. 20).

([8]) Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 (OJ L 122, 24.4.2014, p. 18).

([9]) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218 13.8.2008, p. 82)

Commission delegated regulation on unmanned aircrafts

Commission delegated regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [1], and in particular Article 58 and Article 61 thereof,

Whereas:

(1) The unmanned aircraft systems ('UAS') whose operation presents the lowest risks and that belong to the 'open' category of operations should not be subject to classic aeronautical compliance procedures. The possibility to establish Community harmonisation legislation as referred to in paragraph 6 of Article 56 of Regulation (EU) 2018/1139 should be used for those UAS. Consequently, it is necessary to set out the requirements that address the risks posed by the operation of those UAS, taking full account of other applicable Union harmonisation legislation.

(2) These requirements should cover the essential requirements provided for in Article 55 of Regulation (EU) 2018/1139, in particular as regards the specific features and functionalities necessary to mitigate risks pertaining to the safety of the flight, privacy, and protection of personal data, security or the environment, arising from the operation of these UAS.

(3) When manufacturers place a UAS on the market with the intention to make it available for operations under the 'open' category and therefore affix a class identification label on it, they should ensure compliance of the UAS with the requirements of that class.

(4) Considering the good level of safety achieved by model aircraft already made available on the market, it is appropriate to create the C4 class of UAS which should not be subject to disproportionate technical requirements for the benefit of model aircraft operators.

(5) This Regulation should also apply to UAS, which are considered as toys within the meaning of Directive 2009/48/EC of the European Parliament and of the Council [2]. Those UAS should also comply with Directive 2009/48/EC. That compliance requirement should be taken into account when defining additional safety requirements under this Regulation.

(6) UAS that are not toys within the meaning of Directive 2009/48/EC should comply with the relevant essential health and safety requirements set out in Directive 2006/42/EC of the European Parliament and of the Council [3] in so far as this Directive applies to them, to the extent that those health and safety requirements are not intrinsically linked to the safety of the flight by UAS. Where those health and safety requirements are intrinsically linked to the safety of the flight, only this Regulation should apply.

(7) Directive 2014/30/EU [4] and Directive 2014/53/EU [5] of the European Parliament and of the Council should not apply to unmanned aircraft that are subject to certification according to Regulation (EU) 2018/1139, are exclusively intended for airborne use and intended to be operated only on frequencies allocated by the Radio Regulations of the International Telecommunication Union for protected aeronautical use.

(8) Directive 2014/53/EU should apply to unmanned aircraft that are not subject to certification and are not intended to be operated only on frequencies allocated by the Radio Regulations of the International Telecommunication Union for protected aeronautical use, if they intentionally emit and/or receive electromagnetic waves for the purpose of radio communication and/or radiodetermination at frequencies below 3 000 GHz.

(9) Directive 2014/30/EU should apply to unmanned aircraft that are not subject to certification and are not intended to be operated only on frequencies allocated by the Radio Regulations of the International Telecommunication Union for protected aeronautical use, if they do not fall within the scope of Directive 2014/53/EU.

(10) Decision No 768/2008/EC of the European Parliament and of the Council [6] sets out common principles and horizontal provisions intended to apply to marketing of products that are subject to relevant sectorial legislation. In order to ensure consistency with other sectorial product legislation, the provisions on the marketing of UAS intended to be operated in the 'open' category should be aligned with the framework established by Decision 768/2008/EC.

(11) Directive 2001/95/EC of the European Parliament and of the Council [7] applies to safety risks of UAS so far as there are no specific provisions with the same objective in rules of Union law governing the safety of the products concerned.

(12) This Regulation should apply to all forms of supply, including distance selling.

(13) Member States should take the necessary steps to ensure that UAS intended to be operated in the 'open' category are made available on the market and put into service only where they do not compromise the health and safety of persons, domestic animals or property, when normally used.

(14) In order to provide citizens with high level of environmental protection, it is necessary to limit the noise emissions to the greatest possible extent. Sound power limitations applicable to UAS intended to be operated in the 'open' category might be reviewed at the end of the transitional periods as defined in Commission Implementing Regulation (EU) 2019/947 [8].

(15) Special attention should be paid to ensure compliance of products in the context of an increase of e-commerce. To that end, Member States should be encouraged to pursue cooperation with the competent authorities in third countries and to develop cooperation between market surveillance authorities and customs authorities. Market surveillance authorities should make use, when possible, of the 'notice and action' procedures and establish cooperation with their national authorities competent for the implementation of Directive 2000/31/EC of the European Parliament and of the Council [9]. They should establish close contacts allowing rapid response with key intermediaries that provide hosting services for products sold online.

(16) In order to ensure a high level of protection of public interest, such as health safety, and to guarantee fair competition on the Union market, economic operators should be responsible for the compliance of UAS intended to be operated in the 'open' category with the requirements laid down in this Regulation, in relation to their respective roles in the supply and distribution chain. Therefore, it is necessary to provide a clear and proportionate distribution of obligations, which corresponds to the role of each economic operator in the supply and distribution chain.

(17) In order to facilitate communication between economic operators, national market surveillance authorities and consumers, economic operators supplying or distributing UAS intended to be operated in the 'open' category should provide a website address in addition to the postal address.

(18) The manufacturer, having detailed knowledge of the design and production process, is best placed to carry out the conformity assessment procedure of UAS intended to be operated in

the 'open' category. Conformity assessment should therefore remain solely the obligation of the manufacturer.

(19) This Regulation should apply to any UAS intended to be operated in the 'open' category that is new to the Union market, whether a new UAS made by a manufacturer established in the Union or a new or second-hand UAS imported from a third country.

(20) It is necessary to ensure that UAS from third countries entering the Union market comply with the requirements of this Regulation if they are intended to be operated in the 'open' category. In particular, it should be ensured that manufacturers carry out appropriate conformity assessment procedures. Provision should therefore be made for importers to make sure that the UAS they place on the market comply with the requirements of this Regulation and that they do not place on the market UAS which do not comply with these requirements or present a risk. Provision should also be made for importers to make sure that the conformity assessment procedures have been carried out and that the CE marking and technical documentation drawn up by the manufacturers is available for inspection by the competent national authorities.

(21) The distributor who makes a UAS intended to be operated in the 'open' category available on the market should act with due care to ensure that its handling of the product does not adversely affect its compliance. Both importers and distributors are expected to act with due care in relation to the requirements applicable when placing or making products available on the market.

(22) When placing on the market a UAS intended to be operated in the 'open' category, every importer should indicate on the UAS his name, registered trade name or registered trademark and the address at which he can be contacted. Exceptions should be provided for cases where the size of the UAS does not allow this. This includes cases where the importer would have to open the packaging to put his name and address on the UAS.

(23) Any economic operator that either places a UAS intended to be operated in the 'open' category on the market under his own name or trademark, or modifies a UAS intended to be operated in the 'open' category in such a way that compliance with the applicable requirements may be affected, should be considered to be the manufacturer and should assume the obligations of the manufacturer.

(24) Distributors and importers, being close to the market place, should be involved in market surveillance tasks carried out by the competent national authorities, and should be prepared to participate actively, providing those authorities with all the necessary information relating to the UAS intended to be operated in the 'open' category.

(25) Ensuring the traceability of a UAS intended to be operated in the 'open' category throughout the whole supply chain helps to make market surveillance simpler and more efficient. An efficient traceability system facilitates the market surveillance authorities' task of tracing economic operators who make non-compliant UAS available on the market.

(26) This Regulation should be limited to the setting out of the essential requirements. In order to facilitate the assessment of conformity of UAS intended to be operated in the 'open' category with those requirements, it is necessary to provide for a presumption of conformity for products, which are in conformity with harmonised standards that are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council [10] for the purpose of setting out detailed technical specifications of those requirements.

(27) The essential requirements applicable to UAS intended to be operated in the 'open' category should be worded precisely enough to create legally binding obligations. They should be formulated so as to make it possible to assess conformity with them even in the absence of

harmonised standards or where the manufacturer chooses not to apply a harmonised standard.

(28) Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements of the harmonisation legislation applicable to UAS intended to be operated in the 'open' category under this Regulation. This procedure should apply where appropriate in relation to standards which reference have been published in the Official Journal as providing presumption of conformity with the requirements laid down in this Regulation.

(29) To enable economic operators to demonstrate and the competent authorities to ensure that UAS intended to be operated in the 'open' category made available on the market comply with the essential requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC sets out modules for conformity assessment procedures, which include procedures from the least to the most stringent, in proportion to the level of risk involved and the level of safety required. In order to ensure inter-sectorial coherence and to avoid ad hoc variants of conformity assessment, conformity assessment procedures should be chosen from among those modules.

(30) Market surveillance authorities and UAS operators should have easy access to the EU declaration of conformity. In order to fulfil this requirement, manufacturers should ensure that each UAS intended to be operated in the 'open' category is accompanied either by a copy of the EU declaration of conformity or by the internet address at which the EU declaration of conformity can be accessed.

(31) To ensure effective access to information for market surveillance purposes, the information required to identify all applicable Union acts for UAS intended to be operated in the 'open' category should be available in a single EU declaration of conformity. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.

(32) The CE marking indicating the conformity of a product is the visible consequence of a whole process of conformity assessment in the broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council [11]. Rules governing the affixing of the CE marking to UAS intended to be operated in the 'open' category should be laid in this Regulation.

(33) Some UAS classes intended to be operated in the 'open' category covered by this Regulation require the intervention of conformity assessment bodies. Member States should notify the Commission of these.

(34) It is necessary to ensure a uniformly high level of performance of bodies performing conformity assessments of UAS intended to be operated in the 'open' category throughout the Union, and that all such bodies perform their functions at the same level and under conditions of fair competition. Therefore, obligatory requirements should be set for conformity assessment bodies wishing to be notified in order to provide conformity assessment services.

(35) If a conformity assessment body demonstrates conformity of UAS intended to be operated in the 'open' category with the criteria laid down in harmonised standards, it should be presumed to comply with the corresponding requirements set out in this Regulation.

(36) In order to ensure a consistent level of conformity assessment quality, it is also necessary to set requirements for notifying authorities and other bodies involved in the assessment, notification and monitoring of notified bodies.

(37) Regulation (EC) No 765/2008 sets out rules on the accreditation of conformity assessment bodies, provides a framework for the market surveillance of products and for controls on

products from third countries, and sets out the general principles of the CE marking. The system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008.

(38) Transparent accreditation as provided for in Regulation (EC) No 765/2008, ensuring the necessary level of confidence in certificates of conformity, should be used by national public authorities throughout the Union as the means of demonstrating the technical competence of conformity assessment bodies.

(39) Conformity assessment bodies frequently subcontract parts of their activities linked to the assessment of conformity or have recourse to a subsidiary. In order to safeguard the level of protection required for the UAS intended to be operated in the 'open' category to be placed on the Union market, it is essential that conformity assessment subcontractors and subsidiaries fulfil the same requirements as notified bodies do in relation to the performance of conformity assessment tasks. Therefore, it is important that the assessment of the competence and performance of bodies to be notified, and the monitoring of bodies already notified, also cover activities carried out by subcontractors and subsidiaries.

(40) It is necessary to increase the efficiency and transparency of the notification procedure and, in particular, to adapt it to new technologies so as to enable online notification.

(41) Since notified bodies may offer their services throughout the Union, it is appropriate to give the other Member States and the Commission the opportunity to raise objections concerning a notified body. It is therefore important to provide for a period during which any doubts or concerns as to the competence of conformity assessment bodies can be clarified, before they start operating as notified bodies.

(42) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary administrative burden for economic operators. For the same reason, and also to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. This can best be achieved through appropriate coordination and cooperation between notified bodies.

(43) Interested parties should have the right to appeal against the result of a conformity assessment carried out by a notified body. It is important to ensure that an appeal procedure against all decisions taken by notified bodies is available.

(44) Manufacturers should take all appropriate measures to ensure that UAS intended to be operated in the 'open' category may be placed on the market only if, when properly stored and used for their intended purpose or under conditions, which can be reasonably foreseen, it does not endanger people's health or safety. UAS intended to be operated in the 'open' category should be considered as non-compliant with the essential requirements set out in this Regulation only under conditions of use which can be reasonably foreseen, that is when such use could result from lawful and readily predictable human behaviour.

(45) In order to ensure legal certainty, it is necessary to clarify that the rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EC) No 765/2008, including the provisions regarding the exchange of information through the Rapid Alert System (RAPEX), apply to UAS intended to be operated in the 'open' category. This Regulation should not prevent Member States from choosing the competent authorities to carry out those tasks. In order to ensure a smooth transition as regards the implementation of this Regulation, appropriate transitional measures should be provided.

(46) UAS whose operation present the highest risks should be subject to certification. This Regulation should therefore define the conditions under which the design, production and maintenance of UAS should be subject to certification. Those conditions are linked to a higher

risk of harm to third persons in case of accidents and therefore certification should be required for UAS designed to transport people, UAS designed to transport dangerous goods and for UAS that has any dimension above 3 m and is designed to be operated over assemblies of people. Certification of UAS used in the 'specific' category of operations defined in Implementing Regulation (EU) 2019/947 should also be required if, following a risk assessment, an operational authorisation issued by the competent authority considers that the risk of the operation cannot be adequately mitigated without the certification of the UAS.

(47) UAS placed on the market and intended to be operated in the 'open' category and bearing a class identification label should comply with the certification requirements for UAS operated in the 'specific' or 'certified' categories of operations, as applicable, if those UAS are used outside the 'open' category of operations.

(48) UAS operators that have their principal place of business, are established, or are resident in a third country and that conduct UAS operations within the single European sky airspace should be subject to this Regulation.

(49) The measures provided for in this Regulation are based on Opinion No 01/2018 [12] issued by the European Union Aviation Safety Agency (EASA) in accordance with Article 65 of Regulation (EU) 2018/1139,

HAS ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1. Subject matter

1. This Regulation lays down the requirements for the design and manufacture of unmanned aircraft systems ('UAS') intended to be operated under the rules and conditions defined in Implementing Regulation (EU) 2019/947 and of remote identification add-ons. It also defines the type of UAS whose design, production and maintenance shall be subject to certification.

2. It also establishes rules on making UAS intended for use in the 'open' category and remote identification add-ons available on the market and on their free movement in the Union.

3. This Regulation also lays down rules for third-country UAS operators, when they conduct a UAS operation pursuant to Implementing Regulation (EU) 2019/947 within the single European sky airspace.

Article 2. Scope

1. Chapter II of this Regulation applies to the following products:

(a) UAS intended to be operated under the rules and conditions applicable to the 'open' category of UAS operations pursuant to Implementing Regulation (EU) 2019/947, except privately built UAS, and bearing a class identification label as set out in Parts 1 to 5 of the Annex to this Regulation indicating to which of the five UAS classes referred to in Implementing Regulation (EU) 2019/947 it belongs to;

(b) remote identification add-ons as set out in Part 6 of the Annex to this Regulation.

2. Chapter III of this Regulation applies to UAS operated under the rules and conditions applicable to the 'certified' and 'specific' categories of UAS operations pursuant to Implementing Regulation (EU) 2019/947.

3. Chapter IV of this Regulation applies to UAS operators that have their principal place of business, are established, or reside in a third country, if the UAS are operated in the Union.

4. This Regulation does not apply to UAS intended to be exclusively operated indoors.

Article 3. Definitions
For the purposes of this Regulation, the following definitions apply:

(1)‘unmanned aircraft’ (‘UA’) means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board;

(2)‘equipment to control unmanned aircraft remotely’ means any instrument, equipment, mechanism, apparatus, appurtenance, software or accessory that is necessary for the safe operation of a UA other than a part and which is not carried on board that UA;

(3)‘unmanned aircraft system’ (‘UAS’) means an unmanned aircraft and the equipment to control it remotely;

(4)‘unmanned aircraft system operator’ (‘UAS operator’) means any legal or natural person operating or intending to operate one or more UAS;

(5)‘open’ category' means a category of UAS operations that is defined in Article 4 of Implementing Regulation (EU) 2019/947;

(6)‘specific’ category means a category of UAS operations that is defined in Article 5 of Implementing Regulation (EU) 2019/947;

(7)‘certified’ category means a category of UAS operation that is defined in Article 6 of Implementing Regulation (EU) 2019/947;

(8)‘Union harmonisation legislation’ means any Union legislation harmonising the conditions for placing products on the market;

(9)‘accreditation’ means accreditation as defined in paragraph 10 of Article 2 of Regulation (EC) No 765/2008;

(10)‘conformity assessment’ means the process demonstrating whether the specified requirements relating to a product have been fulfilled;

(11)‘conformity assessment body’ means a body that performs conformity assessment activities including calibration, testing, certification and inspection;

(12)‘CE marking’ means a marking by which the manufacturer indicates that the product is in conformity with the applicable requirements set out in Union harmonisation legislation providing for its affixing;

(13)‘manufacturer’ means any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under their name or trademark;

(14)‘authorised representative’ means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his behalf in relation to specified tasks;

(15)‘importer’ means any natural or legal person established within the Union who places a product from a third country on the Union market;

(16)‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, who makes a product available on the market;

(17)‘economic operators’ means the manufacturer, the authorised representative of the manufacturer, the importer, and the distributor of the UAS;

(18)‘making available on the market’ means any supply of a product for distribution, consumption or use in the Union market in the course of a commercial activity, whether in exchange of payment or free of charge;

(19)‘placing on the market’ means the first making available of a product on the Union market;

(20)‘harmonised standard’ means a harmonised standard as defined in point (c) of Article 2(1) of Regulation (EU) No 1025/2012;

(21)‘technical specification’ means a document that establishes technical requirements to be fulfilled by a product, process or service;

(22)‘privately built UAS’ means a UAS assembled or manufactured for the builder's own use, not including UAS assembled from a set of parts placed on the market by the manufacturer as a single ready-to-assemble kit;

(23)‘market surveillance authority’ means an authority of a Member State responsible for carrying out market surveillance on its territory;

(24)‘recall’ means any measure aimed at achieving the return of a product that has already been made available to the end-user;

(25)‘withdrawal’ means any measure aimed at preventing a product in the supply chain from being made available on the market;

(26)‘single European sky airspace’ means airspace above the territory to which the Treaties apply, as well as any other airspace where Member States apply Regulation (EC) No 551/2004 of the European Parliament and of the Council [13] in accordance with paragraph 3 of Article 1 of that Regulation;

(27)‘remote pilot’ means a natural person responsible for safely conducting the flight of a UA by operating its flight controls, either manually or, when the UA flies automatically, by monitoring its course and remaining able to intervene and change its course at any time;

(28)‘maximum take-off mass’ (‘MTOM’) means the maximum UA mass, including payload and fuel, as defined by the manufacturer or the builder, at which the UA can be operated;

(29)‘payload’ means any instrument, mechanism, equipment, part, apparatus, appurtenance, or accessory, including communications equipment, that is installed in or attached to the aircraft, and is not used or intended to be used in operating or controlling an aircraft in flight, and is not part of an airframe, engine, or propeller;

(30)‘follow-me mode’ means a mode of operation of a UAS where the unmanned aircraft constantly follows the remote pilot within a predetermined radius;

(31)‘direct remote identification’ means a system that ensures the local broadcast of information about a UA in operation, including the marking of the UA, so that this information can be obtained without physical access to the UA;

(32)‘geo-awareness’ means a function that, based on the data provided by Member States, detects a potential breach of airspace limitations and alerts the remote pilots so that they can take effective immediate and action to prevent that breach;

(33)‘sound power level L_{WA}’ means the A-weighted sound power in dB in relation to 1 pW as defined in EN ISO 3744:2010;

(34)‘measured sound power level’ means a sound power level as determined from measurements as laid down in Part 13 of the Annex; measured values may be determined either from a single UA representative for the type of equipment or from the average of a number of UA;

(35)'guaranteed sound power level' means a sound power level determined in accordance with the requirements laid down in Part 13 of the Annex which includes the uncertainties due to production variation and measurement procedures and where the manufacturer, or his authorised representative established in the Community, confirms that according to the technical instruments applied and referred to in the technical documentation it is not exceeded;

(36)'hovering' means staying in the same geographical position in the air;

(37)'assemblies of people' means gatherings where persons are unable to move away due to the density of the people present.

CHAPTER II

UAS intended to be operated in the 'open' category and remote identification add-ons

SECTION 1

Product requirements

Article 4. Requirements

1. The products referred to in paragraph 1 of Article 2 shall meet the requirements set out in Parts 1 to 6 of the Annex.

2. UAS that are not toys within the meaning of Directive 2009/48/EC shall comply with the relevant health and safety requirements set out in Directive 2006/42/EC only in relation to risks other than those linked to the safety of the UA flight.

3. Any updates of software of the products that have already been made available on the market may be made only if such updates do not affect the compliance of the product.

Article 5. **Making available on the market and free movement of products**

1. Products shall only be made available on the market if they satisfy the requirements of this Chapter and do not endanger the health or safety of persons, animals or property.

2. Member States shall not prohibit, restrict or impede, for the aspects covered by this Chapter, the making available on the market of products that comply with this Chapter.

SECTION 2

Obligations of economic operators

Article 6. **Obligations of manufacturers**

1. When placing their product on the Union market, manufacturers shall ensure that it has been designed and manufactured in compliance with the requirements set out in Parts 1 to 6 of the Annex.

2. Manufacturers shall draw up the technical documentation provided for in Article 17 and carry out the relevant conformity assessment procedure referred to in Article 13 or have it outsourced.

Where compliance of the product with the requirements set out in Parts 1 to 6 of the Annex has been demonstrated by that conformity assessment procedure, manufacturers shall draw up an EU declaration of conformity and affix the CE marking.

3. Manufacturers shall keep the technical documentation and the EU declaration of conformity for 10 years after the product has been placed on the market.

4. Manufacturers shall ensure that procedures are in place for series production to remain in conformity with this Chapter. Changes in product design, characteristics or software, and changes in the harmonised standards or in technical specifications by reference to which conformity of a product is declared shall be adequately taken into account.

When deemed appropriate with regard to the risks presented by a product, manufacturers shall, to protect the health and safety of consumers, carry out sample testing of marketed products, investigate, and, if necessary, keep a register of complaints, of non-conforming products and product recalls and shall keep distributors informed of any such monitoring.

5. Manufacturers of UAS shall ensure that the UA bears a type within the meaning of Decision 768/2008/EC and a unique serial number allowing for its identification, and if applicable, compliant with the requirements defined in the corresponding Parts 2 to 4 of the Annex. Manufacturers of remote identification add-ons shall ensure that the remote identification add-on bears a type and a unique serial number allowing for their identification and compliant with the requirements defined in Part 6 of the Annex. In both cases, manufacturers shall ensure that a unique serial number is also affixed to the EU declaration of conformity or to the simplified EU declaration of conformity referred to in Article 14.

6. Manufacturers shall indicate on the product their name, registered trade name or registered trademark, website address and the postal address at which they can be contacted or, where that is not possible, on its packaging, or in a document accompanying it. The address shall indicate a single point at which the manufacturer can be contacted. The contact details shall be indicated in a language easily understood by end-users and market surveillance authorities.

7. Manufacturers shall ensure that the product is accompanied by the manual and information notice required by Parts 1 to 6 of the Annex in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned. Such manual and information notice, as well as any labelling, shall be clear, understandable and legible.

8. Manufacturers shall ensure that each product is accompanied by a copy of the EU declaration of conformity or by a simplified EU declaration of conformity. Where a simplified EU declaration of conformity is provided, it shall contain the exact internet address where the full text of the EU declaration of conformity can be obtained.

9. Manufacturers who consider or have reason to believe that products which they have placed on the market are not in conformity with this Chapter shall immediately take the corrective measures necessary to bring that product into conformity, to withdraw it or recall it, if appropriate. Where the product presents a risk, manufacturers shall immediately inform the market surveillance authorities of the Member States in which they made the product available on the market to that effect, giving details, in particular, of the non-compliance, of any corrective measures taken and of the results thereof.

10. Manufacturers shall, further to a reasoned request from a competent national authority, provide it with all the information and documentation in paper or electronic form necessary to demonstrate the conformity of the product with this Chapter, in a language which can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action taken to eliminate the risks posed by the product which they have placed on the market.

Article 7. **Authorised representatives**

1. A manufacturer may, by a written mandate, appoint an authorised representative.

The obligations laid down in paragraph 1 of Article 6 and the obligation to draw up the technical documentation referred to in paragraph 2 of Article 6 shall not form part of the authorised representative's mandate.

2. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:

(a) keep the EU declaration of conformity and the technical documentation at the disposal of national market surveillance authorities for 10 years after the product has been placed on the Union market;

(b) further to a reasoned request from a market surveillance or border control authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product;

(c) cooperate with the market surveillance or border control authorities, at their request, on any action taken to eliminate the non-conformity of the products covered by the authorised representative's mandate or the safety risks posed by it.

Article 8. **Obligations of importers**

1. Importers shall only place products compliant with the requirements set out in this Chapter on the Union market.

2. Before placing a product on the Union market, importers shall ensure that:

(a) the appropriate conformity assessment procedure referred to in Article 13 has been carried out by the manufacturer;

(b) the manufacturer has drawn up the technical documentation referred to in Article 17;

(c) the product bears the CE marking and, when required, the UA class identification label and the indication of the sound power level;

(d) the product is accompanied by the documents referred to in paragraph 7 and 8 of Article 6;

(e) the manufacturer has complied with the requirements set out in paragraphs 5 and 6 of Article 6.

Where an importer considers or has reasons to believe that a product is not in conformity with the requirements set out in Parts 1 to 6 of the Annex, he shall not place the product on the market until it has been brought into conformity. Furthermore, where the product presents a risk for the health and safety of consumers and third parties, the importer shall inform the manufacturer and the competent national authorities to that effect.

3. Importers shall indicate on the product their name, registered trade name or registered trademark, website and the postal address at which they can be contacted or, where that is not possible, on its packaging or in a document accompanying the product. The contact details shall be in a language easily understood by end-users and market surveillance authorities.

4. Importers shall ensure that the product is accompanied by the manual and information notice required by Parts 1 to 6 of the Annex in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned. That manual and information notice, as well as any labelling, shall be clear, understandable and legible.

5. Importers shall ensure that, while the product is under their responsibility, its storage or transport conditions do not jeopardise its compliance with the requirements set out in Article 4.

6. When deemed appropriate with regard to the risks presented by a product, importers shall, in order to protect the health and safety of end-users and third parties, carry out sample testing of products made available on the market, investigate, and, if necessary, keep a register of

complaints, of non-conforming of products and product recalls, and shall keep distributors informed of any such monitoring.

7. Importers who consider or have reason to believe that a product which they have placed on the market is not in conformity with the applicable Union harmonisation legislation shall immediately take the corrective measures necessary to bring that product into conformity, to withdraw it or recall it, if appropriate. Furthermore, where the product presents a risk, importers shall immediately inform the market surveillance authorities of the Member States in which they made the product available on the market to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken.

8. Importers shall, for 10 years after the product has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.

9. Importers shall, further to a reasoned request from the competent national authority, provide it with all the information and documentation in paper or electronic form necessary to demonstrate the conformity of the product in a language which can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action taken to eliminate the risks posed by the product which they have placed on the market.

Article 9. **Obligations of distributors**

1. When making a product available on the Union market, distributors shall act with due care in relation to the requirements set out in this Chapter.

2. Before making a product available on the market, distributors shall verify that the product bears the CE marking and, when applicable, the UA class identification label and the indication of the sound power level, is accompanied by the documents referred to in paragraphs 7 and 8 of Article 6 and that the manufacturer and the importer have complied with the requirements set out in paragraphs 5 and 6 of Article 6 and in paragraph 3 of Article 8).

Distributors shall ensure that the product is accompanied by the manual and information notice required by Parts 1 to 6 of the Annex in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned. That manual and information notice, as well as any labelling, shall be clear, understandable and legible.

Where a distributor considers or has reason to believe that a product is not in conformity with the requirements set out in Article 4, he shall not make the product available on the market until it has been brought into conformity. Furthermore, where the product presents a risk, the distributor shall inform the manufacturer or the importer to that effect, as well as the competent market surveillance authorities.

3. Distributors shall ensure that, while a product is under their responsibility, its storage or transport conditions do not jeopardise its compliance with the requirements set out in Article 4.

4. Distributors who consider or have reasons to believe that a product which they have made available on the market is not in conformity with the applicable Union harmonisation legislation shall make sure that the corrective measures necessary to bring that product into conformity, to withdraw it or recall it, if appropriate, are taken. Furthermore, where the product presents a risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they made the product available on the market to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken.

5. Distributors shall, further to a reasoned request from the competent national authority, provide it with all the information and documentation in paper or electronic form necessary to demonstrate the conformity of the product. They shall cooperate with that authority, at its

request, on any action taken to eliminate the risks posed by the product which they have made available on the market.

Article 10. **Cases in which obligations of manufacturers apply to importers and distributors**
An importer or distributor shall be considered a manufacturer for the purposes of this Chapter and shall be subject to the obligations of manufacturers pursuant to Article 6, where they place a product on the market under their name or trademark or modify the product already placed on the market in such a way that compliance with this Chapter may be affected.

Article 11. **Identification of economic operators**
1. Economic operators shall, on request, identify the following to the market surveillance authorities:

(a) any economic operator who has supplied them with a product;

(b) any economic operator to whom they have supplied a product.

2. Economic operators shall be able to present the information referred to in paragraph 1:

(a) for 10 years after they have been supplied with the product;

(b) for 10 years after they have supplied the product.

SECTION 3

Conformity of the product

Article 12. **Presumption of conformity**
A product which is in conformity with harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the requirements covered by those standards or parts thereof set out in Parts 1 to 6 of the Annex.

Article 13. **Conformity assessment procedures**
1. The manufacturer shall perform a conformity assessment of the product using one of the following procedures with a view to establishing its compliance with the requirements set out in Parts 1 to 6 of the Annex. The conformity assessment shall take into account all intended and foreseeable operating conditions.

2. The procedures available to conduct the conformity assessment shall be the following:

(a) internal production control as set out in Part 7 of the Annex, when assessing the compliance of a product with the requirements set out in Parts 1, 5 or 6 of the Annex, subject to the condition that the manufacturer has applied harmonised standards, the references of which have been published in the *Official Journal of the European Union*, for all the requirements for which such standards exist;

(b) EU-type examination followed by conformity to type based on internal production control as set out in Part 8 of the Annex;

(c) conformity based on full quality assurance as set out in Part 9 of the Annex, excepted when assessing the compliance of a product which is a toy within the meaning of Directive 2009/48/EC.

Article 14. **EU declaration of conformity**

1. The EU declaration of conformity referred to in paragraph 8 of Article 6 shall state that compliance of the product with the requirements set out in Parts 1 to 6 of the Annex has been demonstrated and, for UAS, identify its class.

2. The EU declaration of conformity shall have the model structure set out in Part 11 of the Annex, shall contain the elements set out in that Part and shall be continuously updated. It shall be translated into the language or languages required by the Member State in which market the product is placed or made available.

3. The simplified EU declaration of conformity referred to in paragraph 8 of Article 6 shall contain the elements set out in Part 12 of the Annex and shall be continuously updated. It shall be translated into the language or languages required by the Member State in which the product is placed or made available on the market. The full text of the EU declaration of conformity shall be available at the internet address referred to in the simplified EU declaration of conformity in a language or languages required by the Member State in which the product is placed or made available on the market.

4. Where a product is subject to more than one Union act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union acts. That declaration shall contain the identification of the Union acts concerned, including their publication references.

5. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product with the requirements laid down in this Chapter.

Article 15. **General principles of the CE marking**

The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

Article 16. **Rules and conditions for affixing the CE marking, the identification number of the notified body, the UAS class identification label and the indication of the sound power level**

1. The CE marking shall be affixed visibly, legibly and indelibly to the product or to the data plate attached to it. Where that is not possible or not warranted on account of the size of the product, it shall be affixed to the packaging.

2. The UA class identification label shall be affixed visibly, legibly and indelibly to the UA and its packaging and shall be at least 5 mm high. The affixing to a product of markings, signs or inscriptions which are likely to mislead third parties regarding the meaning or form of the class identification label shall be prohibited.

3. The indication of the sound power level provided for in Part 14 of the Annex shall be affixed, when applicable, visibly, legibly and indelibly on the UA, unless that is not possible or not warranted on account of the size of the product, and on the packaging.

4. The CE marking and, when applicable, the indication of the sound power level and the UA class identification label shall be affixed before the product is placed on the market.

5. The CE marking shall be followed by the identification number of the notified body where the conformity assessment procedure set out in Part 9 of the Annex is applied.

The identification number of the notified body shall be affixed by the notified body Itself or, under its instructions, by the manufacturer or his authorised representative.

6. Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking.

Article 17. **Technical documentation**

1. The technical documentation shall contain all relevant data and details of the means used by the manufacturer to ensure that the product complies with the requirements set out in Part 1 to 6 of the Annex. It shall, at least, contain the elements set out in Part 10 of the Annex.

2. The technical documentation shall be drawn up before the product is placed on the market and shall be continuously updated.

3. The technical documentation and correspondence relating to any EU-type examination procedure or the assessment of the quality system of the manufacturer shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body.

4. Where the technical documentation does not comply with paragraphs 1, 2 or 3 of this Article, the market surveillance authority may ask the manufacturer or the importer to have a test performed by a body acceptable to the market surveillance authority at the expense of the manufacturer or the importer within a specified period in order to verify compliance of the product with the requirements set out in Parts 1 to 6 of the Annex which applies to it.

SECTION 4

Notification of conformity assessment bodies

Article 18. Notification

Member States shall notify the Commission and the other Member States of bodies authorised to carry out third-party conformity assessment tasks under this Chapter.

Article 19. **Notifying authorities**

1. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, including compliance with Article 24.

2. Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of Regulation (EC) No 765/2008.

3. Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 to a body which is not a governmental entity, that body shall be a legal entity and shall comply mutatis mutandis with the requirements laid down in Article 20. In addition, it shall have arrangements to cover liabilities arising out of its activities.

4. The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3.

Article 20. **Requirements relating to notifying authorities**

1. A notifying authority shall:

(a) be established in such a way that no conflict of interest with conformity assessment bodies occurs;

(b) be organised and operated so as to safeguard the objectivity and impartiality of its activities;

(c) be organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment;

(d) not offer or provide any activities that conformity assessment bodies perform or consultancy services on a commercial or competitive basis;

(e) shall safeguard the confidentiality of the information it obtains;

(f) have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.

Article 21. **Information obligation on notifying authorities**

1. Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes thereto.

2. The Commission shall make that information publicly available.

Article 22. **Requirements relating to notified bodies**

1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 11.

2. A conformity assessment body shall be established under national law of a Member State and have legal personality.

3. A conformity assessment body shall be a third-party body independent of the organisation it assesses.

A body belonging to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of the product which it assesses may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered such a body.

4. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the product which they assess, nor the representative of any of those parties. This shall not preclude the use of the assessed product that is necessary for the operations of the conformity assessment body or the use of such product for personal purposes.

A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of that product, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall, in particular, apply to consultancy services.

Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities,

especially as regards persons or groups of persons with an interest in the results of those activities.

6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it by Part 8 or 9 of the Annex in relation to which it has been notified, whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.

At all times and for each conformity assessment procedure and each kind or category of product in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary:

(a) personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency and the ability of reproduction of those procedures; it shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product in question and the mass or serial nature of the production process.

A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities.

7. The personnel responsible for carrying out conformity assessment tasks shall have the following:

(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;

(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the requirements, of the applicable harmonised standards and of the relevant provisions of Union harmonisation legislation;

(d) the ability to draw up EU-type examination certificates or quality system approvals, records and reports demonstrating that assessments have been carried out.

8. The impartiality of the conformity assessment bodies, their top-level management and of the personnel responsible for carrying out the conformity assessment tasks shall be guaranteed.

The remuneration of the top-level management and of the personnel responsible for carrying out the conformity assessment tasks of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.

9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.

10. The personnel of a conformity assessment body shall observe professional secrecy with regard to all information obtained in carrying out their tasks under Parts 8 and 9 of the Annex or any provision of national law giving effect to them, except in relation to the competent authorities of the Member State in which its activities are carried out. Proprietary rights shall be protected.

11. Conformity assessment bodies shall participate in, or ensure that their personnel responsible for carrying out the conformity assessment tasks are informed of, the relevant standardisation activities, the regulatory activities in the area of UAS and frequency planning, and the activities of the notified body coordination group established under the relevant Union harmonisation legislation and shall apply, as general guidance, the administrative decisions and documents produced as a result of the work of that group.

Article 23. **Presumption of conformity of notified bodies**
Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union*, it shall be presumed to comply with the requirements set out in Article 22 in so far as the applicable harmonised standards cover those requirements.

Article 24. **Subsidiaries of and subcontracting by notified bodies**
1. Where a notified body subcontracts specific tasks connected with conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 22 and shall inform the notifying authority accordingly.

2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries, wherever these are established.

3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the client.

4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under Parts 8 and 9 of the Annex.

Article 25. **Application for notification**
1. A conformity assessment body shall submit an application for notification to the notifying authority of the Member State in which it is established.

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules, and the product for which that body claims to be competent, as well as by an accreditation certificate issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 22.

Article 26. **Notification procedure**
1. Notifying authorities may only notify conformity assessment bodies which have met the requirements laid down in Article 22.

2. They shall notify conformity assessment bodies to the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.

3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules, and the product concerned and the relevant accreditation certification.

4. The body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within 2 weeks of a notification.

5. Only such a body shall be considered a notified body for the purposes of this Chapter.

6. The notifying authority shall notify the Commission and the other Member States of any subsequent relevant changes to the notification.

Article 27. **Identification numbers and lists of notified bodies**

1. The Commission shall assign an identification number to a notified body.

2. It shall assign a single such number even where the body is notified under several Union acts.

3. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been assigned to them and the activities for which they have been notified.

The Commission shall ensure that the list is kept up to date.

Article 28. **Changes to notifications**

1. Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 22, or that it fails to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.

2. In the event of restriction, suspension or withdrawal of the notification, or where the notified body has ceased its activity, the notifying Member State shall take appropriate steps to ensure that the files of that body are either processed by another notified body or kept available for the responsible notifying and market surveillance authorities at their request.

Article 29. **Challenge of the competence of notified bodies**

1. The Commission shall investigate all cases where it has doubts, or doubt is brought to its attention, about the competence of a notified body or the continued fulfilment by a notified body of the requirements and responsibilities to which it is subject.

2. The notifying Member State shall provide the Commission, on request, with all the information relating to the basis for the notification or the maintenance of the competence of the notified body concerned.

3. The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated confidentially.

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including de-notification if necessary.

Article 30. **Operational obligations of notified bodies**

1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided in Parts 8 and 9 of the Annex.

2. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for economic operators. Conformity assessment bodies shall perform their activities taking due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product in question, and the mass or serial nature of the production process.

In doing so, they shall nevertheless respect the degree of rigour and the level of protection required for the compliance of the UA or UAS with this Chapter.

3. Where a notified body finds that the requirements set out in Parts 1 to 6 of the Annex or in corresponding harmonised standards or other technical specifications have not been met by a manufacturer, it shall require the manufacturer to take appropriate corrective measures and shall not issue an EU-type examination certificate or a quality system approval.

4. Where, in the course of the monitoring of conformity following the issue of an EU-type examination certificate or a quality system approval, a notified body finds that a product no longer complies, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the EU-type examination certificate or the quality system approval if necessary.

5. Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any EU-type examination certificates or quality system approvals, as appropriate.

Article 31. **Appeal against decisions of notified bodies**
Notified bodies shall ensure that a transparent and accessible appeal procedure against their decisions is available.

Article 32. **Information obligation on notified bodies**
1. Notified bodies shall inform the notifying authority of the following:

(a) any refusal, restriction, suspension or withdrawal of an EU-type examination certificate or a quality system approval in accordance with the requirements of Parts 8 and 9 of the Annex;

(b) any circumstances affecting the scope of, or conditions for, notification;

(c) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;

(d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

2. Notified bodies shall, in accordance with the requirements of Parts 8 and 9 of the Annex, provide the other bodies notified under this Chapter carrying out similar conformity assessment activities covering the same categories of UA or UAS with the relevant information on issues relating to negative and, on request, positive conformity assessment results.

3. Notified bodies shall fulfil information obligations under Parts 8 and 9 of the Annex.

Article 33. **Exchange of experience**
The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification policy.

Article 34. **Coordination of notified bodies**
1. The Commission shall ensure that appropriate coordination and cooperation between bodies notified under this Chapter are put in place and properly operated in the form of a sectorial group of notified bodies.

2. Notified bodies shall participate in the work of that group, directly of by means of designated representatives.

SECTION 5

Union market surveillance, control of products entering the Union market and Union safeguard procedure

Article 35. **Market surveillance and control of products entering the Union market**
1. Member States shall organise and perform surveillance of the products that are placed on the Union market in accordance with paragraph 3 of Article 15 and Articles 16 to 26 of Regulation (EC) No 765/2008.

2. Member States shall organise and perform control of the products that enter the Union market in accordance with paragraph 5 of Article 15 and Articles 27, 28 and 29 of Regulation (EC) No 765/2008.

3. Member States shall ensure that their market surveillance and border control authorities cooperate with the competent authorities designated under Article 17 of Implementing Regulation (EU) 2019/947 on safety matters and shall establish appropriate communication and coordination mechanisms between them, making the best use of the information contained in the occurrence reporting system defined in Regulation (EU) No 376/2014 of the European Parliament and of the Council [14] and the information systems defined in Articles 22 and 23 of Regulation (EC) No 765/2008.

Article 36. **Procedure for dealing with products presenting a risk at national level**

1. Where the market surveillance authorities of one Member State have taken action pursuant to Article 20 of Regulation (EC) No 765/2008, or where they have sufficient reason to believe that a product presents a risk to the health or safety of persons or to other aspects of public interest protection covered by this Chapter, they shall carry out an evaluation in relation to the product concerned, covering all applicable requirements laid down in this Chapter. The relevant economic operators shall cooperate as necessary with the market surveillance authorities for that purpose.

Where, in the course of the evaluation referred to in the first subparagraph, the market surveillance authorities find that the product does not comply with the requirements laid down in this Chapter, they shall, without delay, require the relevant economic operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw the product from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as they may prescribe.

The market surveillance authorities shall inform the relevant notified body accordingly.

Article 21 of Regulation (EC) No 765/2008 shall apply to the measures referred to in the second subparagraph of this paragraph.

2. Where the market surveillance authorities consider that non-compliance is not restricted to their national territory, they shall inform the Commission and the other Member States of the results of the evaluation and of the actions which they have required the economic operator to take.

3. The economic operator shall ensure that all appropriate corrective action is taken in respect of all products concerned that it has made available on the market throughout the Union.

4. Where the relevant economic operator does not take adequate corrective action within the period referred to in the second subparagraph of paragraph 1, the market surveillance authorities shall take all appropriate provisional measures to prohibit or restrict the product being made available on their national market, to withdraw the product from that market or to recall it.

The market surveillance authorities shall inform the Commission and the other Member States, without delay, of those measures.

5. The information referred to in paragraph 4 shall include all available details, in particular the data necessary for the identification of the non-compliant product, the origin of the product, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant economic operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to either of the following:

(a) failure of the product to meet the requirements set out in Article 4;

(b) shortcomings in the harmonised standards referred to in Article 12.

6. Member States other than the Member State initiating the procedure under this Article shall, without delay, inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product concerned, and, in the event of disagreement with the adopted national measure, of their objections.

7. Where, within three months of receipt of the information referred to in paragraph 5, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified.

8. Member States shall ensure that appropriate restrictive measures, such as withdrawal of the product from the market, are taken in respect of the product concerned without delay.

Article 37. **Union safeguard procedure**

1. Where, on completion of the procedure set out in paragraphs 3 and 4 of Article 36, objections are raised against a measure taken by a Member State, or where the Commission considers a national measure to be contrary to Union legislation, the Commission shall, without delay, enter into consultation with the Member States and the relevant economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not.

The Commission shall address its decision to all Member States and shall immediately communicate it to them and the relevant economic operator or operators.

2. If the national measure is considered justified, all Member States shall take the necessary measures to ensure that the non-compliant product is withdrawn or recalled from their market, and shall inform the Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw that measure.

3. Where the national measure is considered justified and the non-compliance of the product is attributed to shortcomings in the harmonised standards referred to in point (b) of paragraph 5 of Article 36 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

Article 38. **Compliant product which presents a risk**

1. Where, having carried out an evaluation under paragraph 1 of Article 36, a Member State finds that, although the product is in compliance with this Chapter, it presents a risk to the health or safety of persons or to other aspects of public interest protection covered by this Chapter, it shall require the relevant economic operator to take all appropriate measures to ensure that the product concerned, when placed on the market, no longer presents that risk, to withdraw the product from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

2. The economic operator shall ensure that corrective action is taken in respect of all the products concerned that he has made available on the market throughout the Union.

3. The Member State shall immediately inform the Commission and the other Member States. That information shall include all available details, in particular the data necessary for the identification of the product concerned, the origin and the supply chain of product, the nature of the risk involved and the nature and duration of the national measures taken.

4. The Commission shall, without delay, enter into consultation with the Member States and the relevant economic operator or operators and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not and, where necessary, propose appropriate measures.

5. The Commission shall address its decision to all Member States and shall immediately communicate it to them and the relevant economic operator or operators.

Article 39. **Formal non-compliance**

1. Without prejudice to Article 36, where a Member State makes one of the following findings concerning products covered by this Chapter, it shall require the relevant economic operator to put an end to the non-compliance concerned:

(a) the CE marking has been affixed in violation of Article 30 of Regulation (EC) No 765/2008 or of Article 15 or Article 16 of this Regulation;

(b) the CE marking or type has not been affixed;

(c) the identification number of the notified body, where the conformity assessment procedure set out in Part 9 of the Annex is applied, has been affixed in violation of Article 16 or has not been affixed;

(d) the UA class identification label has not been affixed;

(e) the indication of the sound power level if required has not been affixed;

(f) the serial number has not been affixed or has not the correct format;

(g) the manual or the information notice is not available;

(h) the EU declaration of conformity is missing or has not been drawn up;

(i) the EU declaration of conformity has not been drawn up correctly;

(j) technical documentation is either not available or not complete;

(k) manufacturer's or importer's name, registered trade name or registered trademark, website address or postal address are missing.

2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product being made available on the market or ensure that it is withdrawn or recalled from the market.

CHAPTER III

UAS operated in the 'certified' and 'specific' categories

Article 40. **Requirements for UAS operated in the 'certified' and 'specific' categories**

1. The design, production and maintenance of UAS shall be certified if the UAS meets any of the following conditions:

(a) it has a characteristic dimension of 3 m or more, and is designed to be operated over assemblies of people;

(b) it is designed for transporting people;

(c) it is designed for the purpose of transporting dangerous goods and requiring a high level of robustness to mitigate the risks for third parties in case of accident;

(d) it is used in the 'specific' category of operations defined in Article 5 of Implementing Regulation (EU) 2019/947 and the operational authorisation issued by the competent authority, following a risk assessment provided for in Article 11 of Implementing Regulation (EU) 2019/947, considers that the risk of the operation cannot be adequately mitigated without the certification of the UAS.

2. A UAS subject to certification shall comply with the applicable requirements set out in Commission Regulations (EU) No 748/2012 [15], (EU) 2015/640 [16] and (EU) No 1321/2014 [17].

3. Unless it needs to be certified in accordance with paragraph 1, a UAS used in the 'specific' category shall feature the technical capabilities set out in the operational authorisation issued by the competent authority or in the standard scenario defined in Appendix 1 to the Annex of Implementing Regulation (EU) 2019/947 or as defined by the Light UAS Operator Certificate (LUC) pursuant to Part C of the Annex of Implementing Regulation (EU) 2019/947.

CHAPTER IV

Third-country UAS operators

Article 41. **Third-country UAS operators**

1. UAS operators that have their principal place of business, are established, or reside in a third country, shall comply with Implementing Regulation (EU) 2019/947 for the purpose of UAS operations within the single European sky airspace.

2. The competent authority for the third-country UAS operator shall be the competent authority of the first Member State where the UAS operator intends to operate.

3. By way of derogation from paragraph 1, a certificate of the remote pilot competency or UAS operator in accordance with Implementing Regulation (EU) 2019/947, or an equivalent document, may be recognised by the competent authority for the purpose of operation within, to, and out of the Union provided that:

(a) the third country asked for such recognition;

(b) the certificate of the remote pilot competency or the UAS operator's certificate are valid documents of the State of issue; and

(c) the Commission, after consultation of EASA, has ensured that the requirements on the basis of which such certificates have been issued provide the same level of safety as this Regulation does.

CHAPTER V

Final provisions

Article 42. **Entry into force**

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 12 March 2019.

For the Commission

The President

Jean-Claude JUNCKER

---

[1] OJ L 212, 22.8.2018, p. 1.

[2] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1).

([3]) Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24).

([4]) Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (OJ L 96, 29.3.2014, p. 79).

([5]) Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).

([6]) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

(7) Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

(8) Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (see page 45 of this Official Journal).

(9) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(10) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(11) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(12) EASA Opinion No 01/2018 'Introduction of a regulatory framework for the operation of unmanned aircraft systems in the "open" and "specific" categories' (RMT.0230), available at https://www.easa.europa.eu/document-library/opinions

(13) Regulation (EC) No 551/2004 of the European Parliament and of the Council of 10 March 2004 on the organisation and use of the airspace in the single European sky (OJ L 96, 31.3.2004, p. 20).

(14) Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 (OJ L 122, 24.4.2014, p. 18).

(15) Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations (OJ L 224, 21.8.2012, p. 1).

(16) Commission Regulation (EU) 2015/640 of 23 April 2015 on additional airworthiness specifications for a given type of operations and amending Regulation (EU) No 965/2012 (OJ L 106, 24.4.2015, p. 18).

(17) Commission Regulation (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks (OJ L 362, 17.12.2014, p. 1).

Resolution on Autonomous weapon systems

European Parliament resolution of 12 September 2018 on autonomous weapon systems (2018/2752(RSP))

The European Parliament,

– having regard to Title V, Articles 21 and 21(2)(c) of the Treaty on European Union ,

– having regard to the 'Martens clause' included in Protocol 1 of 1977 additional to the Geneva Conventions,

– having regard to Part IV of the UN 2018 Agenda for Disarmament, entitled 'Securing Our Common Future',

– having regard to its study of 3 May 2013 on the human rights implications of the usage of drones and unmanned robots in warfare,

– having regard to its various positions, recommendations and resolutions calling for an international ban on lethal autonomous weapon systems (LAWS), such as its recommendation to the Council of 5 July 2018 on the 73rd session of the United Nations General Assembly[329], the mandate to start negotiations adopted in plenary on 13 March 2018 with a view to the adoption of a regulation of the European Parliament and of the Council establishing the European Defence Industrial Development Programme, its resolution of 13 December 2017 on the Annual Report on Human Rights and Democracy in the World 2016 and the European Union's policy on the matter[330], its recommendation to the Council of 7 July 2016 on the 71st session of the United Nations General Assembly[331], and its resolution of 27 February 2014 on armed drones[332],

– having regard to the annual report of the UN Special Rapporteur on extrajudicial, summary and arbitrary executions, Christof Heyns, of 9 April 2013 (A/HRC/23/47),

– having regard to the EU statements on lethal autonomous weapons systems made to the Group of Governmental Experts of the parties to the Convention on Certain Conventional Weapons in Geneva, at its meetings of 13-17 November 2017, 9-13 April 2018 and 27-31 August 2018,

– having regard to the contributions made by different states, including EU Member States, prior to the 2017 and 2018 meetings of the Group of Governmental Experts,

– having regard to the opinion of the European Economic and Social Committee of 31 May 2017 calling for a human-in-command approach to artificial intelligence and a ban on lethal autonomous weapon systems,

– having regard to the call by the Holy See for a ban on lethal autonomous weapons,

– having regard to the open letter of July 2015 signed by over 3 000 artificial intelligence and robotics researchers and that of 21 August 2017 signed by 116 founders of leading robotics and artificial intelligence companies warning about lethal autonomous weapon systems, and the letter by 240 tech organisations and 3 089 individuals pledging never to develop,

---

329 Texts adopted, P8_TA(2018)0312.
330 Texts adopted, P8_TA(2017)0494.
331 OJ C 101, 16.3.2018, p. 166.
332 OJ C 285, 29.8.2017, p. 110.

produce or use lethal autonomous weapon systems,

– having regard to the statements by the International Committee of the Red Cross and to civil society initiatives such as the Campaign to Stop Killer Robots, which represents 70 organisations in 30 countries, including Human Rights Watch, Article 36, PAX and Amnesty International,

– having regard to Rule 123(2) and (4) of its Rules of Procedure,

A. whereas EU policies and actions are guided by the principles of human rights and respect for human dignity, the principles of the UN Charter and international law; whereas these principles should be applied in order to preserve peace, prevent conflicts and strengthen international security;

B. whereas the term 'lethal autonomous weapon systems' refers to weapon systems without meaningful human control over the critical functions of selecting and attacking individual targets;

C. whereas an unknown number of countries, publicly funded industries and private industries are reportedly researching and developing lethal autonomous weapon systems, ranging all the way from missiles capable of selective targeting to learning machines with cognitive skills to decide whom, when and where to fight;

D. whereas non-autonomous systems such as automated, remotely operated and tele-operated systems should not be considered as lethal autonomous weapons systems;

E. whereas lethal autonomous weapon systems have the potential to fundamentally change warfare by prompting an unprecedented and uncontrolled arms race;

F. whereas the use of lethal autonomous weapon systems raises fundamental ethical and legal questions of human control, in particular with regard to critical functions such as target selection and engagement; whereas machines and robots cannot make human-like decisions involving the legal principles of distinction, proportionality and precaution;

G. whereas human involvement and oversight are central to the lethal decision-making process, since it is humans who remain accountable for decisions concerning life and death;

H. whereas international law, including humanitarian law and human rights law, fully applies to all weapon systems and their operators, and whereas compliance with international law is a key requirement that states must fulfil, particularly when it comes to upholding principles such as protecting the civilian population or taking precautions in attack;

I. whereas the use of lethal autonomous weapon systems raises key questions about the implementation of international human rights law, international humanitarian law and European norms and values with regard to future military actions;

J. whereas in August 2017, 116 founders of leading international robotics and artificial intelligence companies sent an open letter to the UN calling on governments to 'prevent an arms race in these weapons' and 'to avoid the destabilising effects of these technologies';

K. whereas any given lethal autonomous weapon system could malfunction on account of badly written code or a cyber-attack perpetrated by an enemy state or a non-state actor;

L. whereas Parliament has repeatedly called for the urgent development and adoption of a common position on lethal autonomous weapon systems, for an international ban on the

development, production and use of lethal autonomous weapon systems enabling strikes to be carried out without meaningful human control, and for a start to effective negotiations for their prohibition;

1. Recalls the ambition of the EU to be a global actor for peace, and calls for the expansion of its role in global disarmament and non-proliferation efforts, and for its actions and policies to strive for the maintenance of international peace and security, ensuring respect for international humanitarian and human rights law and the protection of civilians and civilian infrastructure;

2. Calls on the Vice-President of the Commission / High Representative for Foreign Affairs and Security Policy (VP/HR), the Member States and the European Council to develop and adopt, as a matter of urgency and prior to the November 2018 meeting of the High Contracting Parties to the Convention on Certain Conventional Weapons, a common position on lethal autonomous weapon systems that ensures meaningful human control over the critical functions of weapon systems, including during deployment, and to speak in relevant forums with one voice and act accordingly; calls, in this context, on the VP/HR, the Member States and the Council to share best practices and garner input from experts, academics and civil society;

3. Urges the VP/HR, the Member States and the Council to work towards the start of international negotiations on a legally binding instrument prohibiting lethal autonomous weapon systems;

4. Stresses, in this light, the fundamental importance of preventing the development and production of any lethal autonomous weapon system lacking human control in critical functions such as target selection and engagement;

5. Recalls its position of 13 March 2018 on the Regulation on the European Defence Industrial Development Programme, in particular paragraph 4 of Article 6 (eligible actions), and underlines its willingness to adopt a similar position in the context of the upcoming defence research programme, the defence industrial development programme and other relevant features of the post-2020 European Defence Fund;

6. Underlines the fact that none of the weapons or weapon systems currently operated by EU forces are lethal autonomous weapon systems; recalls that weapons and weapon systems specifically designed to defend own platforms, forces and populations against highly dynamic threats such as hostile missiles, munitions and aircraft are not considered lethal autonomous weapon systems; emphasises that engagement decisions against human-inhabited aircraft should be taken by human operators;

7. Instructs its President to forward this resolution to the Council, the Commission, the European External Action Service, the governments and parliaments of the Member States, the United Nations and the Secretary-General of NATO.

Standardisation, Certification

Jakub Vostoupal

Introduction

The cybersecurity certification is one of the compliance procedures, which are of a great value to the obliged entities (e.g. under the compliance obligations of the NIS directive). The certification generally speaking means that an unbiased third party assesses the product, service or a process of a manufacturer or other interested party, and evaluates the fulfilment of cybersecurity criteria, usually formulated in a standard or a certification scheme. If these criteria are met, the certification body issues a certificate proving to anybody, that the holder of the certificate was subjected to and passed the evaluation increasing trust in relevant product, service or process in turn.

There are too many cybersecurity standards to be included in this casebook. However, there is at least one, which can be highly recommended to the eager reader – The Common Criteria. It is one of the most advanced international systems, the predecessor and the inspiration for the European legislation.

If anything is to be said about the matter of not-so-well-known cybersecurity certification of products, services and processes in EU, it is surely the fragmentation. Up until now, there was no harmonization of the cybersecurity certification market and legislation in the Union and the only cooperation was the SOG-IS MRA under the Common Criteria system. The problem with this fragmentation was the inability of cross-border recognition of the certificates, so if a manufacturer got a certificate in France according to the French rules, it meant nothing in the Czech Republic and vice versa. In this case, the manufacturer who wanted to sell his products in multiple member states had to undergo several of the certification procedures (which are usually really demanding, both in time and finances required), which excluded many of the SMEs from enjoying the benefits of the single market.

Because of this, the Union adopted a revolutionary piece of legislation, the Cybersecurity Act, which introduces the cybersecurity certification framework. The unification of the cybersecurity certification of products, services and processes with certificates universally recognized all across the Union. Below you can find relevant provisions of Cybersecurity Act and in the section "See also" you shall find the first candidate scheme under this certification framework, the EUCC scheme. The certification framework shall enter into force on June 28, 2021.

The rest of legislation mentioned in this chapter includes the NIS directive and its standardization, and the special certification under the GDPR. There are some other areas, that were left out, because they are still in development, e.g. the cybersecurity certification of the medical equipment.

The Relevant Legislation

Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019, Cybersecurity Act (relevant provisions)

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the functioning of the internal market.

(2) The use of network and information systems by citizens, organisations and businesses across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the internet of Things (IoT) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions. Network and information systems are capable of supporting all aspects of our lives and drive the Union's economic growth. They are the cornerstone for achieving the digital single market.

(3) Increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), as defined in Commission Recommendation 2003/361/EC (4), to operators of critical infrastructure – are better protected from cyber threats.

…

(6) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and would foster mutually reinforcing objectives. Those objectives include further increasing the capabilities and preparedness of Member States and businesses, as well as improving cooperation, information sharing and coordination across Member States and Union institutions, bodies, offices and agencies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in cases of large-scale cross-border incidents and crises, while taking into account the importance of maintaining and further enhancing the national capabilities to respond to cyber threats of all scales.

(7) Additional efforts are also needed to increase citizens', organisations' and businesses' awareness of cybersecurity issues. Moreover, given that incidents undermine trust in digital service providers and in the digital single market itself, especially among consumers, trust should be further strengthened by offering information in a transparent manner on the level of security of ICT products, ICT services and ICT processes that stresses that even a high level of cybersecurity certification cannot guarantee that an ICT product, ICT service or ICT process is completely secure. An increase in trust can be facilitated by Union-wide certification providing for common cybersecurity requirements and evaluation criteria across national markets and sectors.

…

(10) Businesses and individual consumers should have accurate information regarding the assurance level with which the security of their ICT products, ICT services and ICT processes has been certified. At the same time, no ICT product or ICT service is wholly cyber-secure and basic rules of cyber-hygiene have to be promoted and prioritised. Given the growing availability of IoT devices, there is a range of voluntary measures that the private sector can take to reinforce trust in the security of ICT products, ICT services and ICT processes.

(11) Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. In many cases, identifying and documenting such dependencies enables end users of ICT products, ICT services and ICT processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures.

(12) Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation.

(13) Undertakings, organisations and the public sector should configure the ICT products, ICT services or ICT processes designed by them in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible ('security by default'), thereby reducing the burden on users of having to configure an ICT product, ICT service or ICT process appropriately. Security by default should not require extensive configuration or specific technical understanding or non-intuitive behaviour on the part of the user, and should work easily and reliably when implemented. If, on a case-by-case basis, a risk and usability analysis leads to the conclusion that such a setting by default is not feasible, users should be prompted to opt for the most secure setting.

…

(29) With a view to stimulating cooperation between the public and private sector and within the private sector, in particular to support the protection of the critical infrastructures, ENISA should support information sharing within and among sectors, in particular the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available tools and on procedure, as well as by providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral information sharing and analysis centres.

(30) Whereas the potential negative impact of vulnerabilities in ICT products, ICT services and ICT processes is constantly increasing, finding and remedying such vulnerabilities plays an important role in reducing the overall cybersecurity risk. Cooperation between organisations, manufacturers or providers of vulnerable ICT products, ICT services and ICT processes and members of the cybersecurity research community and governments who find vulnerabilities has been proven to significantly increase both the rate of discovery and the remedy of vulnerabilities in ICT products, ICT services and ICT processes. Coordinated vulnerability disclosure specifies a structured process of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organisation the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. The process also provides for coordination between the finder and the organisation as regards the publication of those vulnerabilities. Coordinated vulnerability disclosure policies could play an important role in Member States' efforts to enhance cybersecurity.

…

(48) ENISA should further develop and maintain its expertise on cybersecurity certification with a view to supporting the Union policy in that area. ENISA should build on existing best practices and should promote the uptake of cybersecurity certification within the Union, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level (European cybersecurity certification framework) with a view to increasing the transparency of the cybersecurity assurance of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

(49) Efficient cybersecurity policies should be based on well-developed risk assessment methods, in both the public and private sectors. Risk assessment methods are used at different levels, with no common practice regarding how to apply them efficiently. Promoting and developing best practices for risk assessment and for interoperable risk management solutions in public-sector and private-sector organisations will increase the level of cybersecurity in the Union. To that end, ENISA should support cooperation between stakeholders at Union level and facilitate their efforts relating to the establishment and take-up of European and international standards for risk management and for the measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems.

(50) ENISA should encourage Member States, manufacturers or providers of ICT products, ICT services or ICT processes to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal cybersecurity and should give incentives to do so. In particular, manufacturers and providers of ICT products, ICT services or ICT processes should provide any necessary updates and should recall, withdraw or recycle ICT products, ICT services or ICT processes that do not meet cybersecurity standards, while importers and distributors should make sure that the ICT products, ICT services and ICT processes they place on the Union market comply with the applicable requirements and do not present a risk to Union consumers.

(51) In cooperation with competent authorities, ENISA should be able to disseminate information regarding the level of the cybersecurity of the ICT products, ICT services and ICT processes offered in the internal market, and should issue warnings targeting manufacturers or providers of ICT products, ICT services or ICT processes and requiring them to improve the security of their ICT products, ICT services and ICT processes, including the cybersecurity.

(52) ENISA should take full account of the ongoing research, development and technological assessment activities, in particular those activities carried out by the various Union research initiatives to advise Union institutions, bodies, offices and agencies and where relevant, the Member States at their request, on research needs and priorities in the field of cybersecurity. In order to identify the research needs and priorities, ENISA should also consult the relevant user groups. More specifically, cooperation with the European Research Council, the European Institute for Innovation and Technology and the European Union Institute for Security Studies could be established.

(53) ENISA should regularly consult standardisation organisations, in particular European standardisation organisations, when preparing the European cybersecurity certification schemes.

(54) Cyber threats are a global issue. There is a need for closer international cooperation to improve cybersecurity standards, including the need for definitions of common norms of behaviour, the adoption of codes of conduct, the use of international standards, and information sharing, promoting swifter international collaboration in response to network and information security issues and promoting a common global approach to such issues. To that end, ENISA should support further Union involvement and cooperation with third countries and international organisations by providing the necessary expertise and analysis to the relevant Union institutions, bodies, offices and agencies, where appropriate.

…

(62) The Stakeholder Cybersecurity Certification Group should be established in order to help ENISA and the Commission facilitate the consultation of relevant stakeholders. The Stakeholder Cybersecurity Certification Group should be composed of members representing industry in balanced proportions, both on the demand side and the supply side of ICT products and ICT services, and including, in particular, SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council (16), and academia as well as consumer organisations.

…

(65) Cybersecurity certification plays an important role in increasing trust and security in ICT products, ICT services and ICT processes. The digital single market, and in particular the data economy and the IoT, can thrive only if there is general public trust that such products, services and processes provide a certain level of cybersecurity. Connected and automated cars, electronic medical devices, industrial automation control systems and smart grids are only some examples of sectors in which certification is already widely used or is likely to be used in the near future. The sectors regulated by Directive (EU) 2016/1148 are also sectors in which cybersecurity certification is critical.

(66) In the 2016 Communication ‘Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry’, the Commission outlined the need for high-quality, affordable and interoperable cybersecurity products and solutions. The supply of ICT products, ICT services and ICT processes within the single market remains very fragmented geographically. This is because the cybersecurity industry in Europe has developed largely on the basis of national governmental demand. In addition, the lack of interoperable solutions (technical standards), practices and Union-wide mechanisms of certification are among the other gaps affecting the single market in the field of cybersecurity. This makes it difficult for

European businesses to compete at national, Union and global level. It also reduces the choice of viable and usable cybersecurity technologies that individuals and businesses have access to. Similarly, in the 2017 Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All, the Commission highlighted the need for safe connected products and systems, and indicated that the creation of a European ICT security framework setting rules on how to organise ICT security certification in the Union could both preserve trust in the internet and tackle the current fragmentation of the internal market.

(67) Currently, the cybersecurity certification of ICT products, ICT services and ICT processes is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In that context, a certificate issued by a national cybersecurity certification authority is not in principle recognised in other Member States. Companies thus may have to certify their ICT products, ICT services and ICT processes in several Member States where they operate, for example, with a view to participating in national procurement procedures, which thereby adds to their costs. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach to horizontal cybersecurity issues, for instance in the field of the IoT. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual use, impeding mutual recognition mechanisms within the Union.

(68) Some efforts have been made in order to ensure the mutual recognition of certificates within the Union. However, they have been only partly successful. The most important example in this regard is the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA). While it represents the most important model for cooperation and mutual recognition in the field of security certification, SOG-IS includes only some of the Member States. That fact has limited the effectiveness of SOG-IS MRA from the point of view of the internal market.

(69) Therefore, it is necessary to adopt a common approach and to establish a European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognised and used in all Member States. In doing so, it is essential to build on existing national and international schemes, as well as on mutual recognition systems, in particular SOG-IS, and to make possible a smooth transition from the existing schemes under such systems to schemes under the new European cybersecurity certification framework. The European cybersecurity certification framework should have a twofold purpose. First, it should help increase trust in ICT products, ICT services and ICT processes that have been certified under European cybersecurity certification schemes. Second, it should help avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for undertakings operating in the digital single market. The European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, unless those standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in that regard.

(70) The European cybersecurity certification framework should be established in a uniform manner in all Member States in order to prevent 'certification shopping' based on different levels of stringency in different Member States.

(71) European cybersecurity certification schemes should be built on what already exists at international and national level and, if necessary, on technical specifications from forums and consortia, learning from current strong points and assessing and correcting weaknesses.

(72) Flexible cybersecurity solutions are necessary for the industry to stay ahead of cyber threats, and therefore any certification scheme should be designed in a way that avoids the risk of being outdated quickly.

(73) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products, ICT services and ICT processes. Those schemes should be implemented and supervised by national cybersecurity certification authorities, and certificates issued under those schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or by other private organisations should fall outside of the scope of this Regulation. However, the bodies operating such schemes should be able to propose that the Commission consider such schemes as a basis for approving them as a European cybersecurity certification scheme.

(74) The provisions of this Regulation should be without prejudice to Union law providing specific rules on the certification of ICT products, ICT services and ICT processes. In particular, Regulation (EU) 2016/679 lays down provisions for the establishment of certification mechanisms and of data protection seals and marks, for the purpose of demonstrating the compliance of processing operations by controllers and processors with that Regulation. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of the relevant ICT products, ICT services and ICT processes. This Regulation is without prejudice to the certification of data processing operations under Regulation (EU) 2016/679, including when such operations are embedded in ICT products, ICT services and ICT processes.

(75) The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle. It is not possible to set out in detail the cybersecurity requirements relating to all ICT products, ICT services and ICT processes in this Regulation. ICT products, ICT services and ICT processes and the cybersecurity needs related to those products, services and processes are so diverse that it is very difficult to develop general cybersecurity requirements that are valid in all circumstances. It is therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, which should be complemented by a set of specific cybersecurity objectives that are to be taken into account when designing European cybersecurity certification schemes. The arrangements by which such objectives are to be achieved in specific ICT products, ICT services and ICT processes should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications if no appropriate standards are available.

(76) The technical specifications to be used in European cybersecurity certification schemes should respect the requirements set out in Annex II to Regulation (EU) No 1025/2012 of the European Parliament and of the Council (19). Some deviations from those requirements could, however, be considered to be necessary in duly justified cases where those technical specifications are to be used in a European cybersecurity certification scheme referring to assurance level 'high'. The reasons for such deviations should be made publicly available.

(77) A conformity assessment is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. That procedure is carried out by an independent third party that is not the manufacturer or provider of the ICT products, ICT services or ICT processes that are being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service or ICT process. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out. Depending on the assurance level, the European cybersecurity certification scheme should indicate whether the European cybersecurity certificate is to be issued by a private or public body. Conformity assessment and certification cannot guarantee per se that certified ICT products, ICT services and ICT processes are cyber secure. They are instead procedures and technical methodologies for attesting that ICT products, ICT services and ICT

processes have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example in technical standards.

(78) The choice of the appropriate certification and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services or ICT processes. Accordingly, the assurance level should be commensurate with the level of the risk associated with the intended use of an ICT product, ICT service or ICT process.

(79) European cybersecurity certification schemes could provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes itself carry out all of the checks to ensure that the ICT products, ICT services or ICT processes conform with the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for low complexity ICT products, ICT services or ICT processes that present a low risk to the public, such as simple design and production mechanisms. Moreover, conformity self-assessment should be permitted for ICT products, ICT services or ICT processes only where they correspond to assurance level 'basic'.

(80) European cybersecurity certification schemes could allow for both conformity self-assessments and certifications of ICT products, ICT services or ICT processes. In such a case, the scheme should provide for clear and understandable means for consumers or other users to differentiate between ICT products, ICT services or ICT processes with regard to which the manufacturer or provider of ICT products, ICT services or ICT processes is responsible for the assessment, and ICT products, ICT services or ICT processes that are certified by a third party.

(81) The manufacturer or provider of ICT products, ICT services or ICT processes who carry out a conformity self-assessment should be able to issue and sign the EU statement of conformity as part of the conformity assessment procedure. An EU statement of conformity is a document that states that a specific ICT product, ICT service or ICT process complies with the requirements of the European cybersecurity certification scheme. By issuing and signing the EU statement of conformity, the manufacturer or provider of ICT products, ICT services or ICT processes assumes responsibility for the compliance of the ICT product, ICT service or ICT process with the legal requirements of the European cybersecurity certification scheme. A copy of the EU statement of conformity should be submitted to the national cybersecurity certification authority and to ENISA.

(82) Manufacturers or providers of ICT products, ICT services or ICT processes should make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services or ICT processes with a European cybersecurity certification scheme available to the competent national cybersecurity certification authority for a period provided for in the relevant European cybersecurity certification scheme. The technical documentation should specify the requirements applicable under the scheme and should cover the design, manufacture and operation of the ICT product, ICT service or ICT process to the extent relevant to the conformity self-assessment. The technical documentation should be so compiled as to enable the assessment of whether an ICT product or ICT service complies with the requirements applicable under that scheme.

(83) The governance of the European cybersecurity certification framework takes into account the involvement of Member States as well as the appropriate involvement of stakeholders, and establishes the role of the Commission during the planning and proposing, requesting, preparing, adopting and reviewing of European cybersecurity certification schemes.

(84) The Commission should prepare, with the support of the European Cybersecurity Certification Group (the 'ECCG') and the Stakeholder Cybersecurity Certification Group and after an open and wide consultation, a Union rolling work programme for European cybersecurity

certification schemes and should publish it in the form of a non-binding instrument. The Union rolling work programme should be a strategic document that allows industry, national authorities and standardisation bodies, in particular, to prepare in advance for future European cybersecurity certification schemes. The Union rolling work programme should include a multiannual overview of the requests for candidate schemes which the Commission intends to submit to ENISA for preparation on the basis of specific grounds. The Commission should take into account the Union rolling work programme while preparing its Rolling Plan for ICT Standardisation and standardisation requests to European standardisation organisations. In light of the rapid introduction and uptake of new technologies, the emergence of previously unknown cybersecurity risks, and legislative and market developments, the Commission or the ECCG should be entitled to request ENISA to prepare candidate schemes which have not been included in the Union rolling work programme. In such cases, the Commission and the ECCG should also assess the necessity of such a request, taking into account the overall aims and objectives of this Regulation and the need to ensure continuity as regards ENISA's planning and use of resources.

Following such a request, ENISA should prepare the candidate schemes for specific ICT products, ICT services and ICT processes without undue delay. The Commission should evaluate the positive and negative impact of its request on the specific market in question, especially its impact on SMEs, on innovation, on barriers to entry to that market and on costs to end users. The Commission, on the basis of the candidate scheme prepared by ENISA, should be empowered to adopt the European cybersecurity certification scheme by means of implementing acts. Taking account of the general purpose and security objectives laid down in this Regulation, European cybersecurity certification schemes adopted by the Commission should specify a minimum set of elements concerning the subject matter, scope and functioning of the individual scheme. Those elements should include, among other things, the scope and object of the cybersecurity certification, including the categories of ICT products, ICT services and ICT processes covered, the detailed specification of the cybersecurity requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods, as well as the intended assurance level ('basic', 'substantial' or 'high') and the evaluation levels where applicable. ENISA should be able to refuse a request by the ECCG. Such decisions should be taken by the Management Board and should be duly reasoned.

(85) ENISA should maintain a website providing information on and publicising European cybersecurity certification schemes, which should include, among other things, the requests for the preparation of a candidate scheme as well as the feedback received in the consultation process carried out by ENISA in the preparation phase. The website should also provide information about the European cybersecurity certificates and EU statements of conformity issued under this Regulation including information regarding the withdrawal and expiry of such European cybersecurity certificates and EU statements of conformity. The website should also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

(86) The assurance level of a European certification scheme is a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme. In order to ensure the consistency of the European cybersecurity certification framework, a European cybersecurity certification scheme should be able to specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each European cybersecurity certificate might refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity might only refer to the assurance level 'basic'. The assurance levels would provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service or ICT process and would be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents. Each assurance level should be consistent among the different sectorial domains where certification is applied.

(87) A European cybersecurity certification scheme might specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Evaluation levels should correspond to one of the assurance levels and should be associated with an appropriate combination of assurance components. For all assurance levels, the ICT product, ICT service or ICT process should contain a number of secure functions, as specified by the scheme, which may include: a secure out-of-the-box configuration, a signed code, secure update and exploit mitigations and full stack or heap memory protections. Those functions should have been developed, and be maintained, using security-focused development approaches and associated tools to ensure that effective software and hardware mechanisms are reliably incorporated.

(88) For assurance level 'basic', the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentation of the ICT product, ICT service or ICT process by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product or ICT service should also be subject to the technical review. Where a European cybersecurity certification scheme provides for a conformity self-assessment, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes has carried out a self-assessment of the compliance of the ICT product, ICT service or ICT process with the certification scheme.

(89) For assurance level 'substantial', the evaluation, in addition to the requirements for assurance level 'basic', should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation.

(90) For assurance level 'high', the evaluation, in addition to the requirements for assurance level 'substantial', should be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product, ICT service or ICT process against elaborate cyberattacks performed by persons who have significant skills and resources.

(91) Recourse to European cybersecurity certification and to EU statements of conformity should remain voluntary, unless otherwise provided for in Union law, or in Member State law adopted in accordance with Union law. In the absence of harmonised Union law, Member States are able to adopt national technical regulations providing for mandatory certification under a European cybersecurity certification scheme in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council (20). Member States also have recourse to European cybersecurity certification in the context of public procurement and of Directive 2014/24/EU of the European Parliament and of the Council (21).

(92) In some areas, it could be necessary in the future to impose specific cybersecurity requirements and make the certification thereof mandatory for certain ICT products, ICT services or ICT processes, in order to improve the level of cybersecurity in the Union. The Commission should regularly monitor the impact of adopted European cybersecurity certification schemes on the availability of secure ICT products, ICT services and ICT processes in the internal market and should regularly assess the level of use of the certification schemes by the manufacturers or providers of ICT products, ICT services or ICT processes in the Union. The efficiency of the European cybersecurity certification schemes, and whether specific schemes should be made mandatory, should be assessed in light of the cybersecurity-related legislation of the Union, in particular Directive (EU) 2016/1148, taking into consideration the security of the network and information systems used by operators of essential services.

(93) European cybersecurity certificates and EU statements of conformity should help end users to make informed choices. Therefore, ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued should be accompanied by structured information that is adapted to the expected technical level of the intended end user. All such information should be available online, and, where appropriate, in physical form. The end

user should have access to information regarding the reference number of the certification scheme, the assurance level, the description of the cybersecurity risks associated with the ICT product, ICT service or ICT process, and the issuing authority or body, or should be able to obtain a copy of the European cybersecurity certificate. In addition, the end user should be informed of the cybersecurity support policy, namely for how long the end user can expect to receive cybersecurity updates or patches, of the manufacturer or provider of ICT products, ICT services or ICT processes. Where applicable, guidance on actions or settings that the end user can implement to maintain or increase the cybersecurity of the ICT product or of the ICT service and contact information of a single point of contact to report and receive support in the case of cyberattacks (in addition to automatic reporting) should be provided. That information should be regularly updated and made available on a website providing information on European cybersecurity certification schemes.

(94) With a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for ICT products, ICT services or ICT processes covered by a European cybersecurity certification scheme should cease to be effective from a date established by the Commission by means of implementing acts. Moreover, Member States should not introduce new national cybersecurity certification schemes for ICT products, ICT services or ICT processes already covered by an existing European cybersecurity certification scheme. However, Member States should not be prevented from adopting or maintaining national cybersecurity certification schemes for national security purposes. Member States should inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes. The Commission and the ECCG should evaluate the impact of the new national cybersecurity certification schemes on the proper functioning of the internal market and in light of any strategic interest in requesting a European cybersecurity certification scheme instead.

(95) European cybersecurity certification schemes are intended to help harmonise cybersecurity practices within the Union. They need to contribute to increasing the level of cybersecurity within the Union. The design of the European cybersecurity certification schemes should take into account and allow for the development of innovations in the field of cybersecurity.

(96) European cybersecurity certification schemes should take into account current software and hardware development methods and, in particular, the impact of frequent software or firmware updates on individual European cybersecurity certificates. European cybersecurity certification schemes should specify the conditions under which an update may require that an ICT product, ICT service or ICT process be recertified or that the scope of a specific European cybersecurity certificate be reduced, taking into account any possible adverse effects of the update on compliance with the security requirements of that certificate.

(97) Once a European cybersecurity certification scheme is adopted, manufacturers or providers of ICT products, ICT services or ICT processes should be able to submit applications for certification of their ICT products or ICT services to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a maximum of five years and should be renewable on the same conditions provided that the conformity assessment body still meets the requirements. National accreditation bodies should restrict, suspend or revoke the accreditation of a conformity assessment body where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.

(98) References in national legislation to national standards which have ceased to be effective due to the entry into force of a European cybersecurity certification scheme can be a source of confusion. Therefore, Member States should reflect the adoption of a European cybersecurity certification scheme in their national legislation.

(99) In order to achieve equivalent standards throughout the Union, to facilitate mutual recognition and to promote the overall acceptance of European cybersecurity certificates and EU statements of conformity, it is necessary to put in place a system of peer review between national cybersecurity certification authorities. Peer review should cover procedures for supervising the compliance of ICT products, ICT services and ICT processes with European cybersecurity certificates, for monitoring the obligations of manufacturers or providers of ICT products, ICT services or ICT processes who carry out the conformity self-assessment, for monitoring conformity assessment bodies, as well as the appropriateness of the expertise of the staff of bodies issuing certificates for assurance level 'high'. The Commission should be able, by means of implementing acts, to establish at least a five-year plan for peer reviews, as well as lay down criteria and methodologies for the operation of the peer review system.

(100) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the European cybersecurity certification framework, certain European cybersecurity certification schemes may include a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services and ICT processes with an assurance level 'high' under such schemes. The ECCG should support the implementation of such peer-assessment mechanisms. The peer assessments should assess in particular whether the bodies concerned carry out their tasks in a harmonised way, and may include appeal mechanisms. The results of the peer assessments should be made publicly available. The bodies concerned may adopt appropriate measures to adapt their practices and expertise accordingly.

(101) Member States should designate one or more national cybersecurity certification authorities to supervise compliance with obligations arising from this Regulation. A national cybersecurity certification authority may be an existing or new authority. A Member State should also be able to designate, after agreeing with another Member State, one or more national cybersecurity certification authorities in the territory of that other Member State.

(102) National cybersecurity certification authorities should in particular monitor and enforce the obligations of manufacturers or providers of ICT products, ICT services or ICT processes established in its respective territory in relation to the EU statement of conformity, should assist the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies by providing them with expertise and relevant information, should authorise conformity assessment bodies to carry out their tasks where such bodies meet additional requirements set out in a European cybersecurity certification scheme, and should monitor relevant developments in the field of cybersecurity certification. National cybersecurity certification authorities should also handle complaints lodged by natural or legal persons in relation to European cybersecurity certificates issued by those authorities or in relation to European cybersecurity certificates issued by conformity assessment bodies, where such certificates indicate assurance level 'high', should investigate, to the extent appropriate, the subject matter of the complaint and should inform the complainant of the progress and the outcome of the investigation within a reasonable period. Moreover, national cybersecurity certification authorities should cooperate with other national cybersecurity certification authorities or other public authorities, including by the sharing of information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with specific European cybersecurity certification schemes. The Commission should facilitate that sharing of information by making available a general electronic information support system, for example the Information and Communication System on Market Surveillance (ICSMS) and the Rapid Alert System for dangerous non-food products (RAPEX), already used by market surveillance authorities pursuant to Regulation (EC) No 765/2008.

(103) With a view to ensuring the consistent application of the European cybersecurity certification framework, an ECCG that consists of representatives of national cybersecurity certification authorities or other relevant national authorities should be established. The main

tasks of the ECCG should be to advise and assist the Commission in its work towards ensuring the consistent implementation and application of the European cybersecurity certification framework, to assist and closely cooperate with ENISA in the preparation of candidate cybersecurity certification schemes, in duly justified cases to request ENISA to prepare a candidate scheme, to adopt opinions addressed to ENISA on candidate schemes and to adopt opinions addressed to the Commission on the maintenance and review of existing European cybersecurity certifications schemes. The ECCG should facilitate the exchange of good practices and expertise between the various national cybersecurity certification authorities that are responsible for the authorisation of conformity assessment bodies and the issuance of European cybersecurity certificates.

(104) In order to raise awareness and to facilitate the acceptance of future European cybersecurity certification schemes, the Commission may issue general or sector-specific cybersecurity guidelines, for example on good cybersecurity practices or responsible cybersecurity behaviour highlighting the positive effect of the use of certified ICT products, ICT services and ICT processes.

(105) In order to further facilitate trade, and recognising that ICT supply chains are global, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). The Commission, taking into account the advice from ENISA and the European Cybersecurity Certification Group, may recommend the opening of relevant negotiations. Each European cybersecurity certification scheme should provide specific conditions for such mutual recognition agreements with third countries.

(106) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (22).

(107) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT products, ICT services or ICT processes, for the adoption of implementing acts on arrangements for carrying out inquiries by ENISA, for the adoption of implementing acts on a plan for the peer review of national cybersecurity certification authorities, as well as for the adoption of implementing acts on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national cybersecurity certification authorities to the Commission.

(108) ENISA's operations should be subject to regular and independent evaluation. That evaluation should have regard to ENISA's objectives, its working practices and the relevance of its tasks, in particular its tasks relating to the operational cooperation at Union level. That evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework. In the event of a review, the Commission should evaluate how ENISA's role as a reference point for advice and expertise can be reinforced and should also evaluate the possibility of a role for ENISA in supporting the assessment of third country ICT products, ICT services and ICT processes that do not comply with Union rules, where such products, services and processes enter the Union.

(109) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(110) Regulation (EU) No 526/2013 should be repealed,

HAVE ADOPTED THIS REGULATION:

TITLE I

GENERAL PROVISIONS

Article 1. Subject matter and scope

1. With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:

(a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and

(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

The framework referred to in point (b) of the first subparagraph applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.

2. This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law.

Article 2. Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(2) 'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;

(3) 'national strategy on the security of network and information systems' means a national strategy on the security of network and information systems as defined in point (3) of Article 4 of Directive (EU) 2016/1148;

(4) 'operator of essential services' means an operator of essential services as defined in point (4) of Article 4 of Directive (EU) 2016/1148;

(5) 'digital service provider' means a digital service provider as defined in point (6) of Article 4 of Directive (EU) 2016/1148;

(6) 'incident' means an incident as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

(7) 'incident handling' means incident handling as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

(8) 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(9) 'European cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

(10)'national cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme;

(11) 'European cybersecurity certificate' means a document issued by a relevant body, attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;

(12) 'ICT product' means an element or a group of elements of a network or information system;

(13) 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

(14) 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

(15) 'accreditation' means accreditation as defined in point (10) of Article 2 of Regulation (EC) No 765/2008;

(16) 'national accreditation body' means a national accreditation body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008;

(17) 'conformity assessment' means a conformity assessment as defined in point (12) of Article 2 of Regulation (EC) No 765/2008;

(18) 'conformity assessment body' means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008;

(19) 'standard' means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012;

(20) 'technical specification' means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service or ICT process;

(21) 'assurance level' means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned;

(22) 'conformity self-assessment' means an action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.

...

Article 22. Stakeholder Cybersecurity Certification Group

1. The Stakeholder Cybersecurity Certification Group shall be established.

2. The Stakeholder Cybersecurity Certification Group shall be composed of members selected from among recognised experts representing the relevant stakeholders. The Commission, following a transparent and open call, shall select, on the basis of a proposal from ENISA, members

of the Stakeholder Cybersecurity Certification Group ensuring a balance between the different stakeholder groups as well as an appropriate gender and geographical balance.

3. The Stakeholder Cybersecurity Certification Group shall:

(a) advise the Commission on strategic issues regarding the European cybersecurity certification framework;

(b) upon request, advise ENISA on general and strategic matters concerning ENISA's tasks relating to market, cybersecurity certification, and standardisation;

(c) assist the Commission in the preparation of the Union rolling work programme referred to in Article 47;

(d) issue an opinion on the Union rolling work programme pursuant to Article 47(4); and

(e) in urgent cases, provide advice to the Commission and the ECCG on the need for additional certification schemes not included in the Union rolling work programme, as outlined in Articles 47 and 48.

4. The Stakeholder Certification Group shall be co-chaired by the representatives of the Commission and of ENISA, and its secretariat shall be provided by ENISA.

TITLE III

CYBERSECURITY CERTIFICATION FRAMEWORK

Article 46. European cybersecurity certification framework

1. The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes.

2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle.

Article 47. The Union rolling work programme for European cybersecurity certification

1. The Commission shall publish a Union rolling work programme for European cybersecurity certification (the 'Union rolling work programme') that shall identify strategic priorities for future European cybersecurity certification schemes.

2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.

3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:

(a) the availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services or ICT processes and, in particular, as regards the risk of fragmentation;

(b) relevant Union or Member State law or policy;

(c) market demand;

(d) developments in the cyber threat landscape;

(e) request for the preparation of a specific candidate scheme by the ECCG.

4. The Commission shall take due account of the opinions issued by the ECCG and the Stakeholder Certification Group on the draft Union rolling work programme.

5. The first Union rolling work programme shall be published by 28 June 2020. The Union rolling work programme shall be updated at least once every three years and more often if necessary.

Article 48. Request for a European cybersecurity certification scheme

1. The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme.

2. In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. The Union rolling work programme shall be updated accordingly.

Article 49. Preparation, adoption and review of a European cybersecurity certification scheme

1. Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54.

2. Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board.

3. When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.

4. For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise.

5. ENISA shall closely cooperate with the ECCG. The ECCG shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme and shall adopt an opinion on the candidate scheme.

6. ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme prepared in accordance with paragraphs 3, 4 and 5 to the Commission. The opinion of the ECCG shall not bind ENISA, nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission.

7. The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes which meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

8. At least every five years, ENISA shall evaluate each adopted European cybersecurity certification scheme, taking into account the feedback received from interested parties. If necessary, the Commission or the ECCG may request ENISA to start the process of developing a revised candidate scheme in accordance with Article 48 and this Article.

Article 50. Website on European cybersecurity certification schemes

1. ENISA shall maintain a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information provided in accordance with Article 55.

2. Where applicable, the website referred to in paragraph 1 shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

Article 51. Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:

(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;

(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;

(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

(d) to identify and document known dependencies and vulnerabilities;

(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;

(i) that ICT products, ICT services and ICT processes are secure by default and by design;

(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

Article 52. Assurance levels of European cybersecurity certification schemes

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.

2. European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity certification scheme under which the European cybersecurity certificate or EU statement of conformity is issued.

3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service or ICT process is to undergo.

4. The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.

5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level 'basic' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

6. A European cybersecurity certificate that refers to assurance level 'substantial' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

7. A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.

8. A European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Each of the evaluation levels shall correspond to one of the assurance levels and shall be defined by an appropriate combination of assurance components.

Article 53. Conformity self-assessment

1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.

2. The manufacturer or provider of ICT products, ICT services or ICT processes may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products,

ICT services or ICT processes shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme.

3. The manufacturer or provider of ICT products, ICT services or ICT processes shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products or ICT services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

4. The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.

5. EU statements of conformity shall be recognised in all Member States.

Article 54. Elements of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall include at least the following elements:

(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;

(b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;

(c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

(d) where applicable, one or more assurance levels;

(e) an indication of whether conformity self-assessment is permitted under the scheme;

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;

(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;

(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;

(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;

(l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;

(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;

(n) where applicable, rules concerning the retention of records by conformity assessment bodies;

(o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;

(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;

(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;

(r) maximum period of validity of European cybersecurity certificates issued under the scheme;

(s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;

(t) conditions for the mutual recognition of certification schemes with third countries;

(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;

(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

2. The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law.

3. Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.

4. In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

Article 55. Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes

1. The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information:

(a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;

(b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;

(c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

(d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.

2. The information referred to in paragraph 1 shall be available in electronic form and shall remain available and be updated as necessary at least until the expiry of the corresponding European cybersecurity certificate or EU statement of conformity.

Article 56. Cybersecurity certification

1. ICT products, ICT services and ICT processes that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme.

2. The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.

3. The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services and ICT processes covered by an existing certification scheme which are to be covered by a mandatory certification scheme.

As a priority, the Commission shall focus on the sectors listed in Annex II to Directive (EU) 2016/1148, which shall be assessed at the latest two years after the adoption of the first European cybersecurity certification scheme.

When preparing the assessment the Commission shall:

(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services or ICT processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services or ICT processes;

(b) take into account the existence and implementation of relevant Member State and third country law;

(c) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;

(d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services or ICT processes, including SMEs;

(e) propose the most speedy and efficient way in which the transition from a voluntary to mandatory certification schemes is to be implemented.

4. The conformity assessment bodies referred to in Article 60 shall issue European cybersecurity certificates pursuant to this Article referring to assurance level 'basic' or 'substantial' on the basis of criteria included in the European cybersecurity certification scheme adopted by the Commission pursuant to Article 49.

5. By way of derogation from paragraph 4, in duly justified cases a European cybersecurity certification scheme may provide that European cybersecurity certificates resulting from that scheme are to be issued only by a public body. Such body shall be one of the following:

(a) a national cybersecurity certification authority as referred to in Article 58(1); or

(b) a public body that is accredited as a conformity assessment body pursuant to Article 60(1).

6. Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level 'high', the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body:

(a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or

(b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

7. The natural or legal person who submits ICT products, ICT services or ICT processes for certification shall make available to the national cybersecurity certification authority referred to in Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.

8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service or ICT process that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned.

9. A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met.

10. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.

Article 57. National cybersecurity certification schemes and certificates

1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are not covered by a European cybersecurity certification scheme shall continue to exist.

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services and ICT processes already covered by a European cybersecurity certification scheme that is in force.

3. Existing certificates that were issued under national cybersecurity certification schemes and are covered by a European cybersecurity certification scheme shall remain valid until their expiry date.

4. With a view to avoiding the fragmentation of the internal market, Member States shall inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes.

Article 58. National cybersecurity certification authorities

1. Each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, shall designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State.

2. Each Member State shall inform the Commission of the identity of the designated national cybersecurity certification authorities. Where a Member State designates more than one authority, it shall also inform the Commission about the tasks assigned to each of those authorities.

3. Without prejudice to point (a) of Article 56(5) and Article 56(6), each national cybersecurity certification authority shall be independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making.

4. Member States shall ensure that the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in this Article and that those activities are carried out independently from each other.

5. Member States shall ensure that national cybersecurity certification authorities have adequate resources to exercise their powers and to carry out their tasks in an effective and efficient manner.

6. For the effective implementation of this Regulation, it is appropriate that national cybersecurity certification authorities participate in the ECCG in an active, effective, efficient and secure manner.

7. National cybersecurity certification authorities shall:

(a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;

(b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services or ICT processes that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;

(c) without prejudice to Article 60(3), actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;

(d) monitor and supervise the activities of the public bodies referred to in Article 56(5);

(e) where applicable, authorise conformity assessment bodies in accordance with Article 60(3) and restrict, suspend or withdraw existing authorisation where conformity assessment bodies infringe the requirements of this Regulation;

(f) handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6) or in relation

to EU statements of conformity issued under Article 53, and shall investigate the subject matter of such complaints to the extent appropriate, and shall inform the complainant of the progress and the outcome of the investigation within a reasonable period;

(g) provide an annual summary report on the activities conducted under points (b), (c) and (d) of this paragraph or under paragraph 8 to ENISA and the ECCG;

(h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; and

(i) monitor relevant developments in the field of cybersecurity certification.

8. Each national cybersecurity certification authority shall have at least the following powers:

(a) to request conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires for the performance of its tasks;

(b) to carry out investigations, in the form of audits, of conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity, for the purpose of verifying their compliance with this Title;

(c) to take appropriate measures, in accordance with national law, to ensure that conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity comply with this Regulation or with a European cybersecurity certification scheme;

(d) to obtain access to the premises of any conformity assessment bodies or holders of European cybersecurity certificates, for the purpose of carrying out investigations in accordance with Union or Member State procedural law;

(e) to withdraw, in accordance with national law, European cybersecurity certificates issued by the national cybersecurity certification authorities or European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6), where such certificates do not comply with this Regulation or with a European cybersecurity certification scheme;

(f) to impose penalties in accordance with national law, as provided for in Article 65, and to require the immediate cessation of infringements of the obligations set out in this Regulation.

9. National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services and ICT processes.

Article 59. Peer review

1. With a view to achieving equivalent standards throughout the Union in respect of European cybersecurity certificates and EU statements of conformity, national cybersecurity certification authorities shall be subject to peer review.

2. Peer review shall be carried out on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints.

3. Peer review shall assess:

(a) where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point

(a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in Article 58 and whether those activities are carried out independently from each other;

(b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services and ICT processes with European cybersecurity certificates pursuant to point (a) of Article 58(7);

(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services or ICT processes pursuant to point (b) of Article 58(7);

(d) the procedures for monitoring, authorising and supervising the activities of the conformity assessment bodies;

(e) where applicable, whether the staff of authorities or bodies that issue certificates for assurance level 'high' pursuant to Article 56(6) have the appropriate expertise.

4. Peer review shall be carried out by at least two national cybersecurity certification authorities of other Member States and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review.

5. The Commission may adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it. In adopting those implementing acts, the Commission shall take due account of the views of the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

6. The outcomes of peer reviews shall be examined by the ECCG, which shall draw up summaries that may be made publicly available and which shall, where necessary, issue guidelines or recommendations on actions or measures to be taken by the entities concerned.

Article 60. Conformity assessment bodies

1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.

2. Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to point (a) of Article 56(5) and Article 56(6), the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1 of this Article.

3. Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes.

4. The accreditation referred to in paragraph 1 shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed on the same conditions, provided that the conformity assessment body still meets the requirements set out in this Article. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.

Article 61. Notification

1. For each European cybersecurity certification scheme, the national cybersecurity certification authorities shall notify the Commission of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 60(3) to issue European cybersecurity certificates at specified assurance levels as referred to in Article 52. The national cybersecurity certification authorities shall notify the Commission of any subsequent changes thereto without undue delay.

2. One year after the entry into force of a European cybersecurity certification scheme, the Commission shall publish a list of the conformity assessment bodies notified under that scheme in the Official Journal of the European Union.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish the amendments to the list of notified conformity assessment bodies in the Official Journal of the European Union within two months of the date of receipt of that notification.

4. A national cybersecurity certification authority may submit to the Commission a request to remove a conformity assessment body notified by that authority from the list referred to in paragraph 2. The Commission shall publish the corresponding amendments to that list in the Official Journal of the European Union within one month of the date of receipt of the national cybersecurity certification authority's request.

5. The Commission may adopt implementing acts to establish the circumstances, formats and procedures for notifications referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

Article 62. European Cybersecurity Certification Group

1. The European Cybersecurity Certification Group (the 'ECCG') shall be established.

2. The ECCG shall be composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG shall not represent more than two Member States.

3. Stakeholders and relevant third parties may be invited to attend meetings of the ECCG and to participate in its work.

4. The ECCG shall have the following tasks:

(a) to advise and assist the Commission in its work to ensure the consistent implementation and application of this Title, in particular regarding the Union rolling work programme, cybersecurity certification policy issues, the coordination of policy approaches, and the preparation of European cybersecurity certification schemes;

(b) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme pursuant to Article 49;

(c) to adopt an opinion on candidate schemes prepared by ENISA pursuant to Article 49;

(d) to request ENISA to prepare candidate schemes pursuant to Article 48(2);

(e) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;

(f) to examine relevant developments in the field of cybersecurity certification and to exchange information and good practices on cybersecurity certification schemes;

(g) to facilitate the cooperation between national cybersecurity certification authorities under this Title through capacity-building and the exchange of information, in particular by

establishing methods for the efficient exchange of information relating to issues concerning cybersecurity certification;

(h) to support the implementation of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to point (u) of Article 54(1);

(i) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including by reviewing existing European cybersecurity certification schemes and, where appropriate, making recommendations to ENISA to engage with relevant international standardisation organisations to address insufficiencies or gaps in available internationally recognised standards.

5. With the assistance of ENISA, the Commission shall chair the ECCG, and the Commission shall provide the ECCG with a secretariat in accordance with point (e) of Article 8(1).

Article 63. Right to lodge a complaint

1. Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body when acting in accordance with Article 56(6), with the relevant national cybersecurity certification authority.

2. The authority or body with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken, and shall inform the complainant of the right to an effective judicial remedy referred to in Article 64.

Article 64. Right to an effective judicial remedy

1. Notwithstanding any administrative or other non-judicial remedies, natural and legal persons shall have the right to an effective judicial remedy with regard to:

(a) decisions taken by the authority or body referred to in Article 63(1) including, where applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons;

(b) a failure to act on a complaint lodged with the authority or body referred to in Article 63(1).

2. Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.

Article 65. Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall without delay notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.

TITLE IV

FINAL PROVISIONS

Article 66. Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, point (b) of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 67. Evaluation and review

1. By 28 June 2024, and every five years thereafter, the Commission shall evaluate the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification. The evaluation shall take into account any feedback provided to ENISA in response to its activities. Where the Commission considers that the continued operation of ENISA is no longer justified in light of the objectives, mandate and tasks assigned to it, the Commission may propose that this Regulation be amended with regard to the provisions related to ENISA.

2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III of this Regulation with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improving the functioning of the internal market.

3. The evaluation shall assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services and ICT processes which do not meet basic cybersecurity requirements from entering the Union market.

4. By 28 June 2024, and every five years thereafter, the Commission shall transmit a report on the evaluation together with its conclusions to the European Parliament, to the Council and to the Management Board. The findings of that report shall be made public.

Article 68. Repeal and succession

1. Regulation (EU) No 526/2013 is repealed with effect from 27 June 2019.

2. References to Regulation (EU) No 526/2013 and to the ENISA as established by that Regulation shall be construed as references to this Regulation and to ENISA as established by this Regulation.

3. ENISA as established by this Regulation shall succeed ENISA as established by Regulation (EU) No 526/2013 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities. All decisions of the Management Board and the Executive Board adopted in accordance with Regulation (EU) No 526/2013 shall remain valid, provided that they comply with this Regulation.

4. ENISA shall be established for an indefinite period as of 27 June 2019.

5. The Executive Director appointed pursuant to Article 24(4) of Regulation (EU) No 526/2013 shall remain in office and exercise the duties of the Executive Director as referred to in Article 20 of this Regulation for the remaining part of the Executive Director's term of office. The other conditions of his or her contract shall remain unchanged.

6. The members of the Management Board and their alternates appointed pursuant to Article 6 of Regulation (EU) No 526/2013 shall remain in office and exercise the functions of the Management Board as referred to in Article 15 of this Regulation for the remaining part of their term of office.

Article 69. Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. Articles 58, 60, 61, 63, 64 and 65 shall apply from 28 June 2021.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 17 April 2019.

1.3 ANNEX – Requirements to be met by the Conformity Assessment Bodies

Conformity assessment bodies that wish to be accredited shall meet the following requirements:

1. A conformity assessment body shall be established under national law and shall have legal personality.

2. A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services or ICT processes that it assesses.

3. A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services or ICT processes which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.

4. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes.

5. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of the ICT products, ICT services or ICT processes which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services.

6. If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented.

7. Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

8. Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities.

9. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other

things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.

10. At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services or ICT processes, a conformity assessment body shall have at its disposal the necessary:

(a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process.

11. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment and facilities.

12. The persons responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all conformity assessment activities;

(b) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the applicable requirements and testing standards;

(d) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.

13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed.

14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.

15. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment.

16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.

17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification.

18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.

19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes.

20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.

Directive (EU 2016/1148 of European Parliament and of the Council of 6 July 2016, the NIS Directive (relevant provisions

Directive (EU 2016/1148 of European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

...

(66) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level. ENISA should assist Member States through advice and guidelines. To this end, it might be helpful to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council

CHAPTER IV

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14. Security requirements and incident notification

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

(a) the number of users affected by the disruption of the essential service;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident.

5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.

At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.

6. After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

7. Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.

CHAPTER V

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS

Article 16. Security requirements and incident notification

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) monitoring, auditing and testing;

(e) compliance with international standards.

2. Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.

3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

(e) the extent of the impact on economic and societal activities.

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

5. Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.

6. Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall,

in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

7. After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

8. The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017.

9. The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

10. Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.

11. Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC (19).

CHAPTER VI

STANDARDISATION AND VOLUNTARY NOTIFICATION

Article 19. Standardisation

1. In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

Regulation (EU 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation (relevant provisions

Regulation (EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

...

Article 40. Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41. Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42. Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43. Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent

pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

See also

Common Criteria base European candidate cybersecurity certification scheme, accessible here: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/

ICT security certification opportunities in the healthcare sector, accessible here: https://www.enisa.europa.eu/publications/healthcare-certification

Digital Discovery

Jan Kolouch

Data retention

1. Introduction

The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.

Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR had been presented as a necessary measure.

It was perceived as necessary, that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.

For not only the above-mentioned reasons has been adopted:

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=CS

Date of document: 15/03/2006

Date of effect: 03/05/2006;

Date of transposition: 15/09/2007;

Date of end of validity: 08/04/2014; See 62012CJ0293

Article 1. **Subject matter and scope**

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2. Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (7), and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

(a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user;

(b) 'user' means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

(c) 'telephone service' means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(d) 'user ID' means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

(e) 'cell ID' means the identity of the cell from which a mobile telephony call originated or in which it terminated;

(f) 'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3. **Obligation to retain data**

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the

communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4. **Access to data**
Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5. **Categories of data to be retained**
1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2)concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii)the user ID and telephone number allocated to any communication entering the public telephone network;

(iii)the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1)concerning fixed network telephony and mobile telephony:

(i)the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii)the name(s) and address(es) of the subscriber(s) or registered user(s);

(2)concerning Internet e-mail and Internet telephony:

(i)the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii)the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c)data necessary to identify the date, time and duration of a communication:

(1)concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2)concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6. **Periods of retention**

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7. **Data protection and data security**

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a)the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b)the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c)the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d)the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8. **Storage requirements for retained data**
Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9. **Supervisory authority**
1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10. Statistics
1. Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include:

- the cases in which information was provided to the competent authorities in accordance with applicable national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,
- the cases where requests for data could not be met.

2. Such statistics shall not contain personal data.

Article 11. **Amendment of Directive 2002/58/EC**
The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

'1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (8) to be retained for the purposes referred to in Article 1(1) of that Directive.

Aricle 12. **Future measures**
1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That

Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.

2. The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.

3. Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13. **Remedies, liability and penalties**

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14. Evaluation

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Article 15. Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007. They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

3. Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the Official Journal of the European Union.

Article 16. **Entry into force**

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 17. Addressees
This Directive is addressed to the Member States.

Done at Strasbourg, 15 March 2006.

2. Judgments of courts on data retention

Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung (C-594/12)

JUDGMENT OF THE COURT (Grand Chamber) 8 April 2014 (*1) 'Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union'In Joined Cases C-293/12 and C-594/12

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&from=CS

Case C-293/12

On 11 August 2006, Digital Rights brought an action before the High Court in which it claimed that it owned a mobile phone which had been registered on 3 June 2006 and that it had used that mobile phone since that date. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications and asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State.

The High Court, considering that it was not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined, decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1.Is the restriction on the rights of the [p]laintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 … and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:

(a)Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime?

and/or

(b) Ensuring the proper functioning of the internal market of the European Union?

2.Specifically,

(i)Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?

(ii)Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union ("the Charter")] and Article 8 ECHR?

(iii)Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv)Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v)Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?

3.To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?'

Case C–594/12

The origin of the request for a preliminary ruling in Case C-594/12 lies in several actions brought before the Verfassungsgerichtshof by the Kärntner Landesregierung and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants, respectively, seeking the annulment of Paragraph 102a of the 2003 Law on telecommunications (Telekommunikationsgesetz 2003), which was inserted into that 2003 Law by the federal law amending it (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) for the purpose of transposing Directive 2006/24 into Austrian national law. They take the view, inter alia, that

Article 102a of the Telekommunikationsgesetz 2003 infringes the fundamental right of individuals to the protection of their data.

The Verfassungsgerichtshof wonders, in particular, whether Directive 2006/24 is compatible with the Charter in so far as it allows the storing of many types of data in relation to an unlimited number of persons for a long time. The Verfassungsgerichtshof takes the view that the retention of data affects almost exclusively persons whose conduct in no way justifies the retention of data relating to them. Those persons are exposed to a greater risk that authorities will investigate the data relating to them, become acquainted with the content of those data, find out about their private lives and use those data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months. According to the referring court, there are doubts as to whether that directive is able to achieve the objectives which it pursues and as to the proportionality of the interference with the fundamental rights concerned.

In those circumstances the Verfassungsgerichtshof decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1.Concerning the validity of acts of institutions of the European Union:

Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?

2.Concerning the interpretation of the Treaties:

(a) In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and Regulation (EC) No 45/2001 of the European Parliament and of the Council [of 18 December 2000] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ 2001 L 8, p. 1] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

(b) What is the relationship between "Union law", as referred to in the final sentence of Article 52(3) of the Charter, and the directives in the field of the law on data protection?

(c) In view of the fact that [Directive 95/26] and Regulation … No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

(d) Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

(e) Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?'

Interference with the rights laid down in Articles 7 and 8 of the Charter

By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, as the Advocate

General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.

To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 75).

As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.

Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., Leander v. Sweden, 26 March 1987, § 48, Series A no 116; Rotaru v. Romania [GC], no. 28341/95, § 46, ECHR 2000-V; and Weber and Saravia v. Germany (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.

It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter

Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the

provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.

It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v Council and Commission EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P Al-Aqsa v Council EU:C:2012:711, paragraph 130). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C-145/09 Tsakouridis EU:C:2010:708, paragraphs 46 and 47). Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

In those circumstances, it is necessary to verify the proportionality of the interference found to exist.

In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, to that effect, Case C-343/09 Afton Chemical EU:C:2010:419, paragraph 45; Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10 Nelson and Others EU:C:2012:657, paragraph 71; Case C-283/11 Sky Österreich EU:C:2013:28, paragraph 50; and Case C-101/12 Schaible EU:C:2013:661, paragraph 29).

With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).

In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the

interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General has pointed out in paragraph 137 of his Opinion.

As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).

In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.

Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).

The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, S. and Marper v. the United Kingdom, § 103, and M. K. v. France, 18 April 2013, no. 19522/09, § 35).

As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3

of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).

Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.

Consequently, the answer to the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12 is that Directive 2006/24 is invalid.

The first question and the second question, parts (a) and (e), and the third question in Case C-293/12 and the second question in Case C-594/12

It follows from what was held in the previous paragraph that there is no need to answer the first question, the second question, parts (a) and (e), and the third question in Case C-293/12 or the second question in Case C-594/12.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

Tele2 Sverige AB (C-203/15) and **Secretary of State for the Home Department (C-698/15)**

JUDGMENT OF THE COURT (Grand Chamber) 21 December 2016 (*) (Reference for a preliminary ruling — Electronic communications — Processing of personal data — Confidentiality of electronic communications — Protection — Directive 2002/58/EC — Articles 5, 6 and 9 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — National legislation — Providers of electronic communications services — Obligation relating to the general and indiscriminate retention of traffic and location data — National authorities — Access to data — No prior review by a court or independent administrative authority — Compatibility with EU law) In Joined Cases C-203/15 and C-698/15

http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN

Case C-203/15

On 9 April 2014, Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the PTS that, following the ruling in the judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12; 'the *Digital Rights* judgment', EU:C:2014:238) that Directive 2006/24 was invalid, it would cease, as from 14 April 2014, to retain electronic communications data, covered by the LEK, and that it would erase data retained prior to that date.

On 15 April 2014, the Rikspolisstyrelsen (the Swedish National Police Authority, Sweden) sent to the PTS a complaint to the effect that Tele2 Sverige had ceased to send to it the data concerned.

On 29 April 2014, the justitieminister (Swedish Minister for Justice) appointed a special reporter to examine the Swedish legislation at issue in the light of the *Digital Rights* judgment. In a report dated 13 June 2014, entitled 'Datalagring, EU-rätten och svensk rätt, Ds 2014:23' (Data retention, EU law and Swedish law; 'the 2014 report'), the special reporter concluded that the national legislation on the retention of data, as set out in Paragraphs 16a to 16f of the LEK, was not incompatible with either EU law or the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 ('the ECHR'). The special reporter emphasised that the *Digital Rights* judgment could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle. From his perspective, neither should the *Digital Rights* judgment be understood as meaning that the Court had established, in that judgment, a set of criteria all of which had to be satisfied if legislation was to be able to be regarded as proportionate. He considered that it was necessary to assess all the circumstances in order to determine the compatibility of the Swedish legislation with EU law, such as the extent of data retention in the light of the provisions on access to data, on the duration of retention, and on the protection and the security of data.

On that basis, on 19 June 2014 the PTS informed Tele2 Sverige that it was in breach of its obligations under the national legislation in failing to retain the data covered by the LEK for six months, for the purpose of combating crime. By an order of 27 June 2014, the PTS ordered Tele2 Sverige to commence, by no later than 25 July 2014, the retention of that data.

Tele2 Sverige considered that the 2014 report was based on a misinterpretation of the *Digital Rights* judgment and that the obligation to retain data was in breach of the fundamental rights guaranteed by the Charter, and therefore brought an action before the Förvaltningsrätten i

Stockholm (Administrative Court, Stockholm) challenging the order of 27 June 2014. Since that court dismissed the action, by judgment of 13 October 2014, Tele2 Sverige brought an appeal against that judgment before the referring court.

In the opinion of the referring court, the compatibility of the Swedish legislation with EU law should be assessed with regard to Article 15(1) of Directive 2002/58. While that directive establishes the general rule that traffic and location data should be erased or made anonymous when no longer required for the transmission of a communication, Article 15(1) of that directive introduces a derogation from that general rule since it permits the Member States, where justified on one of the specified grounds, to restrict that obligation to erase or render anonymous, or even to make provision for the retention of data. Accordingly, EU law allows, in certain situations, the retention of electronic communications data.

The referring court nonetheless seeks to ascertain whether a general and indiscriminate obligation to retain electronic communications data, such as that at issue in the main proceedings, is compatible, taking into consideration the *Digital Rights* judgment, with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Given that the opinions of the parties differ on that point, it is necessary that the Court give an unequivocal ruling on whether, as maintained by Tele2 Sverige, the general and indiscriminate retention of electronic communications data is per se incompatible with Articles 7 and 8 and Article 52(1) of the Charter, or whether, as stated in the 2014 Report, the compatibility of such retention of data is to be assessed in the light of provisions relating to access to the data, the protection and security of the data and the duration of retention.

In those circumstances the Kammarrätten i Stockholm (Administrative Court of Appeal of Stockholm, Sweden) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

'(1) Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime … compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

(2) If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:

(a) access by the national authorities to the retained data is determined as [described in paragraphs 19 to 36 of the order for reference], and

(b) data protection and security requirements are regulated as [described in paragraphs 38 to 43 of the order for reference], and

(c) all relevant data is to be retained for six months, calculated as from the day when the communication is ended, and subsequently erased as [described in paragraph 37 of the order for reference]?'

Case C-698/15

Mr Watson, Mr Brice and Mr Lewis each lodged, before the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) (United Kingdom), applications for judicial review of the legality of Section 1 of DRIPA, claiming, inter alia, that that section is incompatible with Articles 7 and 8 of the Charter and Article 8 of the ECHR.

By judgment of 17 July 2015, the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) held that the *Digital Rights* judgment laid down 'mandatory requirements of EU law' applicable to the legislation of Member States on the retention of communications data and

access to such data. According to the High Court of Justice, since the Court, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. It follows from the underlying logic of the *Digital Rights* judgment that legislation that establishes a general body of rules for the retention of communications data is in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, Section 1 of DRIPA is not compatible with Articles 7 and 8 of the Charter in so far as it does not lay down clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an independent administrative body.

The Secretary of State for the Home Department brought an appeal against that judgment before the Court of Appeal (England & Wales) (Civil Division) (United Kingdom).

That court states that Section 1(1) of DRIPA empowers the Secretary of State for the Home Department to adopt, without any prior authorisation from a court or an independent administrative body, a general regime requiring public telecommunications operators to retain all data relating to any postal service or any telecommunications service for a maximum period of 12 months if he/she considers that such a requirement is necessary and proportionate to achieve the purposes stated in the United Kingdom legislation. Even though that data does not include the content of a communication, it could be highly intrusive into the privacy of users of communications services.

In the order for reference and in its judgment of 20 November 2015, delivered in the appeal procedure, wherein it decided to send to the Court this request for a preliminary ruling, the referring court considers that the national rules on the retention of data necessarily fall within the scope of Article 15(1) of Directive 2002/58 and must therefore conform to the requirements of the Charter. However, as stated in Article 1(3) of that directive, the EU legislature did not harmonise the rules relating to access to retained data.

As regards the effect of the *Digital Rights* judgment on the issues raised in the main proceedings, the referring court states that, in the case that gave rise to that judgment, the Court was considering the validity of Directive 2006/24 and not the validity of any national legislation. Having regard, inter alia, to the close relationship between the retention of data and access to that data, it was essential that that directive should incorporate a set of safeguards and that the *Digital Rights* judgment should analyse, when examining the lawfulness of the data retention regime established by that directive, the rules relating to access to that data. The Court had not therefore intended to lay down, in that judgment, mandatory requirements applicable to national legislation on access to data that does not implement EU law. Further, the reasoning of the Court was closely linked to the objective pursued by Directive 2006/24. National legislation should, however, be assessed in the light of the objectives pursued by that legislation and its context.

As regards the need to refer questions to the Court for a preliminary ruling, the referring court draws attention to the fact that, when the order for reference was issued, six courts in other Member States, five of those courts being courts of last resort, had declared national legislation to be invalid on the basis of the *Digital Rights* judgment. The answer to the questions referred is therefore not obvious, although the answer is required to give a ruling on the cases brought before that court.

In those circumstances, the Court of Appeal (England & Wales) (Civil Division) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

'(1) Does [the *Digital Rights* judgment] (including, in particular, paragraphs 60 to 62 thereof) lay down mandatory requirements of EU law applicable to a Member State's domestic regime

governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of [the Charter]?

(2) Does [the *Digital Rights* judgment] expand the scope of Articles 7 and/or 8 of [the Charter] beyond that of Article 8 of the European Convention of Human Rights … as established in the jurisprudence of the European Court of Human Rights …?'

Consideration of the questions referred for a preliminary ruling

The first question in Case C-203/15

By the first question in Case C-203/15, the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm) seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation such as that at issue in the main proceedings that provides, for the purpose of fighting crime, for general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications.

That question arises, in particular, from the fact that Directive 2006/24, which the national legislation at issue in the main proceedings was intended to transpose, was declared to be invalid by the *Digital Rights* judgment, though the parties disagree on the scope of that judgment and its effect on that legislation, given that it governs the retention of traffic and location data and access to that data by the national authorities.

It is necessary first to examine whether national legislation such as that at issue in the main proceeding falls within the scope of EU law.

The scope of Directive 2002/58

The Member States that have submitted written observations to the Court have differed in their opinions as to whether and to what extent national legislation on the retention of traffic and location data and access to that data by the national authorities, for the purpose of combating crime, falls within the scope of Directive 2002/58. Whereas, in particular, the Belgian, Danish, German and Estonian Governments, Ireland and the Netherlands Government have expressed the opinion that the answer is that it does, the Czech Government has proposed that the answer is that it does not, since the sole objective of such legislation is to combat crime. The United Kingdom Government, for its part, argues that only legislation relating to the retention of data, but not legislation relating to the access to that data by the competent national law enforcement authorities, falls within the scope of that directive.

As regards, finally, the Commission, while it maintained, in its written observations submitted to the Court in Case C-203/15, that the national legislation at issue in the main proceedings falls within the scope of Directive 2002/58, the Commission argues, in its written observations in Case C-698/15, that only national rules relating to the retention of data, and not those relating to the access of the national authorities to that data, fall within the scope of that directive. The latter rules should, however, according to the Commission, be taken into consideration in order to assess whether national legislation governing the retention of data by providers of electronic communications services constitutes a proportionate interference in the fundamental rights guaranteed in Articles 7 and 8 of the Charter.

In that regard, it must be observed that a determination of the scope of Directive 2002/58 must take into consideration, inter alia, the general structure of that directive.

Article 1(1) of Directive 2002/58 indicates that the directive provides, inter alia, for the harmonisation of the provisions of national law required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and

confidentiality, with respect to the processing of personal data in the electronic communications sector.

Article 1(3) of that directive excludes from its scope 'activities of the State' in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters (see, by analogy, with respect to the first indent of Article 3(2) of Directive 95/46, judgments of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 43, and of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, paragraph 41).

Article 3 of Directive 2002/58 states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices ('electronic communications services'). Consequently, that directive must be regarded as regulating the activities of the providers of such services.

Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, 'legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 [of that directive]'. The second sentence of Article 15(1) of that directive identifies, as an example of measures that may thus be adopted by Member States, measures 'providing for the retention of data'.

Admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 51). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive.

However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.

Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services. Accordingly, Article 15(1), read together with Article 3 of that directive, must be interpreted as meaning that such legislative measures fall within the scope of that directive.

The scope of that directive extends, in particular, to a legislative measure, such as that at issue in the main proceedings, that requires such providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data.

The scope of that directive also extends to a legislative measure relating, as in the main proceedings, to the access of the national authorities to the data retained by the providers of electronic communications services.

The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons

other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including 'any data related to such communications', in order to protect the confidentiality of electronic communications.

In those circumstances, a legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services, for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that directive.

Further, since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services.

That interpretation is confirmed by Article 15(1b) of Directive 2002/58, which provides that providers are to establish internal procedures for responding to requests for access to users' personal data, based on provisions of national law adopted pursuant to Article 15(1) of that directive.

It follows from the foregoing that national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15, falls within the scope of Directive 2002/58.

The interpretation of Article 15(1) of Directive 2002/58, in the light of Articles 7, 8, 11 and Article 52(1) of the Charter

It must be observed that, according to Article 1(2) of Directive 2002/58, the provisions of that directive 'particularise and complement' Directive 95/46. As stated in its recital 2, Directive 2002/58 seeks to ensure, in particular, full respect for the rights set out in Articles 7 and 8 of the Charter. In that regard, it is clear from the explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which led to Directive 2002/58, that the EU legislature sought 'to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used'.

To that end, Directive 2002/58 contains specific provisions designed, as is apparent from, in particular, recitals 6 and 7 of that directive, to offer to the users of electronic communications services protection against risks to their personal data and privacy that arise from new technology and the increasing capacity for automated storage and processing of data.

In particular, Article 5(1) of that directive provides that the Member States must ensure, by means of their national legislation, the confidentiality of communications effected by means of a public communications network and publicly available electronic communications services, and the confidentiality of the related traffic data.

The principle of confidentiality of communications established by Directive 2002/58 implies, inter alia, as stated in the second sentence of Article 5(1) of that directive, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 47).

Accordingly, as confirmed by recitals 22 and 26 of Directive 2002/58, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and

for the time necessary for the billing and marketing of services and the provision of value added services (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraphs 47 and 48). As regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers obtained.

The scope of Article 5, Article 6 and Article 9(1) of Directive 2002/58, which seek to ensure the confidentiality of communications and related data, and to minimise the risks of misuse, must moreover be assessed in the light of recital 30 of that directive, which states: 'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'.

Admittedly, Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to in Articles 6 and 9 of that directive (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 50).

Nonetheless, in so far as Article 15(1) of Directive 2002/58 enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision must, in accordance with the Court's settled case-law, be interpreted strictly (see, by analogy, judgment of 22 November 2012, *Probst*, C-119/12, EU:C:2012:748, paragraph 23). That provision cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless.

It must, in that regard, be observed that the first sentence of Article 15(1) of Directive 2002/58 provides that the objectives pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be 'to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system', or one of the other objectives specified in Article 13(1) of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 53). That list of objectives is exhaustive, as is apparent from the second sentence of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on 'the grounds laid down' in the first sentence of Article 15(1) of that directive. Accordingly, the Member States cannot adopt such measures for purposes other than those listed in that latter provision.

Further, the third sentence of Article 15(1) of Directive 2002/58 provides that '[a]ll the measures referred to [in Article 15(1)] shall be in accordance with the general principles of [European Union] law, including those referred to in Article 6(1) and (2) [EU]', which include the general principles and fundamental rights now guaranteed by the Charter. Article 15(1) of Directive 2002/58 must, therefore, be interpreted in the light of the fundamental rights guaranteed by the Charter (see, by analogy, in relation to Directive 95/46, judgments of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 68, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 38).

In that regard, it must be emphasised that the obligation imposed on providers of electronic communications services, by national legislation such as that at issue in the main proceedings, to retain traffic data in order, when necessary, to make that data available to the competent national

authorities, raises questions relating to compatibility not only with Articles 7 and 8 of the Charter, which are expressly referred to in the questions referred for a preliminary ruling, but also with the freedom of expression guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraphs 25 and 70).

Accordingly, the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 of the Charter, as derived from the Court's case-law (see, to that effect, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 39 and the case-law cited), must be taken into consideration in interpreting Article 15(1) of Directive 2002/58. The same is true of the right to freedom of expression in the light of the particular importance accorded to that freedom in any democratic society. That fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 12 June 2003, *Schmidberger*, C-112/00, EU:C:2003:333, paragraph 79, and of 6 September 2011, *Patriciello*, C-163/10, EU:C:2011:543, paragraph 31).

In that regard, it must be recalled that, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 50).

With respect to that last issue, the first sentence of Article 15(1) of Directive 2002/58 provides that Member States may adopt a measure that derogates from the principle of confidentiality of communications and related traffic data where it is a 'necessary, appropriate and proportionate measure within a democratic society', in view of the objectives laid down in that provision. As regards recital 11 of that directive, it states that a measure of that kind must be 'strictly' proportionate to the intended purpose. In relation to, in particular, the retention of data, the requirement laid down in the second sentence of Article 15(1) of that directive is that data should be retained 'for a limited period' and be 'justified' by reference to one of the objectives stated in the first sentence of Article 15(1) of that directive.

Due regard to the principle of proportionality also derives from the Court's settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary (judgments of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 77; the *Digital Rights* judgment, paragraph 52, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 92).

As regards whether national legislation, such as that at issue in Case C-203/15, satisfies those conditions, it must be observed that that legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. As stated in the order for reference, the categories of data covered by that legislation correspond, in essence, to the data whose retention was required by Directive 2006/24.

The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia,

the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (see, by analogy, with respect to Directive 2006/24, the *Digital Rights* judgment, paragraph 26).

That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the *Digital Rights judgment*, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.

The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 37).

Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 39), the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 28).

Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 60).

Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 51).

In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.

Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an

indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraphs 57 and 58).

Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 59).

National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 54 and the case-law cited).

Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of

fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

The second question in Case C-203/15 and the first question in Case C-698/15

It must, at the outset, be noted that the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm) referred the second question in Case C-203/15 only in the event that the answer to the first question in that case was negative. That second question, however, arises irrespective of whether retention of data is generalised or targeted, as set out in paragraphs 108 to 111 of this judgment. Accordingly, the Court must answer the second question in Case C-203/15 together with the first question in Case C-698/15, which is referred regardless of the extent of the obligation to retain data that is imposed on providers of electronic communications services.

By the second question in Case C-203/15 and the first question in Case C-698/15, the referring courts seek, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data, and more particularly, the access of the competent national authorities to retained data, where that legislation does not restrict that access solely to the objective of fighting serious crime, where that access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

As regards objectives that are capable of justifying national legislation that derogates from the principle of confidentiality of electronic communications, it must be borne in mind that, since, as stated in paragraphs 90 and 102 of this judgment, the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, access to the retained data must correspond, genuinely and strictly, to one of those objectives. Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data.

As regards compatibility with the principle of proportionality, national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data must ensure, in accordance with what was stated in paragraphs 95 and 96 of this judgment, that such access does not exceed the limits of what is strictly necessary.

Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, 'be subject to adequate safeguards', a data retention measure must, as follows from the case-law cited in paragraph 109 of this judgment, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.

In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 61).

Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly

necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (see, by analogy, ECtHR, 4 December 2015, *Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.

In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary*, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80).

Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 95).

With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraphs 66 to 68).

In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the *Digital Rights* judgment, paragraph 68, and the judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraphs 41 and 58).

It is the task of the referring courts to determine whether and to what extent the national legislation at issue in the main proceedings satisfies the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as set out in paragraphs 115 to 123 of this judgment, with respect to both the access of the competent national authorities to the retained data and the protection and level of security of that data.

Having regard to all of the foregoing, the answer to the second question in Case C-203/15 and to the first question in Case C-698/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

The second question in Case C-698/15

By the second question in Case C-698/15, the Court of Appeal (England & Wales) (Civil Division) seeks in essence to ascertain whether, in the *Digital Rights* judgment, the Court interpreted Articles 7 and/or 8 of the Charter in such a way as to expand the scope conferred on Article 8 ECHR by the European Court of Human Rights.

As a preliminary point, it should be recalled that, whilst, as Article 6(3) TEU confirms, fundamental rights recognised by the ECHR constitute general principles of EU law, the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law (see, to that effect, judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 45 and the case-law cited).

Accordingly, the interpretation of Directive 2002/58, which is at issue in this case, must be undertaken solely in the light of the fundamental rights guaranteed by the Charter (see, to that effect, judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 46 and the case-law cited).

Further, it must be borne in mind that the explanation on Article 52 of the Charter indicates that paragraph 3 of that article is intended to ensure the necessary consistency between the Charter and the ECHR, 'without thereby adversely affecting the autonomy of Union law and … that of the Court of Justice of the European Union' (judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 47). In particular, as expressly stated in the second sentence of Article 52(3) of the Charter, the first sentence of Article 52(3) does not preclude Union law from providing protection that is more extensive then the ECHR. It should be added, finally, that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.

However, in accordance with the Court's settled case-law, the justification for making a request for a preliminary ruling is not for advisory opinions to be delivered on general or hypothetical questions, but rather that it is necessary for the effective resolution of a dispute concerning EU law (see, to that effect, judgments of 24 April 2012, *Kamberaj*, C-571/10, EU:C:2012:233, paragraph 41; of 26 February 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 42, and of 27 February 2014, *Pohotovosť*, C-470/12, EU:C:2014:101 paragraph 29).

In this case, in view of the considerations set out, in particular, in paragraphs 128 and 129 of the present judgment, the question whether the protection conferred by Articles 7 and 8 of the Charter is wider than that guaranteed in Article 8 of the ECHR is not such as to affect the interpretation of Directive 2002/58, read in the light of the Charter, which is the matter in dispute in the proceedings in Case C-698/15.

Accordingly, it does not appear that an answer to the second question in Case C-698/15 can provide any interpretation of points of EU law that is required for the resolution, in the light of that law, of that dispute.

It follows that the second question in Case C-698/15 is inadmissible.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.**

2. **Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.**

3. **The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible.**

Ireland (C-301/06)

Case C-301/06 Ireland v European Parliament and Council of the European Union (Action for annulment – Directive 2006/24/EC – Retention of data generated or processed in connection with the provision of electronic communications services – Choice of legal basis)

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62006CJ0301

Background to the dispute

On 28 April 2004, the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland submitted to the Council of the European Union a proposal for a framework decision to be adopted on the basis of Articles 31(1)(c) EU and 34(2)(b) EU. The subject of that proposal was the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data in public communication networks for the purposes of the prevention, investigation, detection and prosecution of criminal offences, including terrorism (Council Document 8958/04).

The Commission of the European Communities stated that it favoured the legal basis used in that proposed framework decision with respect to a part of it. In particular, it pointed out that Article 47 EU did not allow an instrument based on the EU Treaty to affect the *acquis communautaire*, in this case Directives 95/46 and 2002/58. Taking the view that the determination of the categories of data to be retained and of the relevant retention period fell within the competence of the Community legislature, the Commission reserved the right to submit a proposal for a directive.

On 21 September 2005, the Commission adopted a proposal, based on Article 95 EC, for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication[s] services and amending Directive 2002/58 [COM(2005) 438 final].

During its session on 1 and 2 December 2005, the Council decided to seek the adoption of a directive based on the EC Treaty, rather than pursuing the adoption of a framework decision.

On 14 December 2005, the European Parliament delivered its opinion in accordance with the co-decision procedure under Article 251 EC.

The Council adopted Directive 2006/24 by qualified majority at its session on 21 February 2006. Ireland and the Slovak Republic voted against the adoption of that directive.

Forms of order sought by the parties

Ireland claims that the Court should:

- annul Directive 2006/24 on the ground that it was not adopted on an appropriate legal basis, and
- order the Council and the Parliament to pay the costs.

The Parliament contends that the Court should:

– primarily, dismiss the action as unfounded, and

– order Ireland to pay all the costs of the present proceedings,

– or, in the alternative, should the Court annul Directive 2006/24, declare that the effects of that directive are to remain in force until a new measure enters into force.

The Council contends that the Court should:

– dismiss the action brought by Ireland, and

– order Ireland to pay the costs.

By orders of 1 February 2007, the President of the Court granted leave to the Slovak Republic to intervene in support of the form of order sought by Ireland and to the Kingdom of Spain, the Kingdom of the Netherlands, the Commission and the European Data Protection Supervisor to intervene in support of the forms of order sought by the Parliament and the Council.

Findings of the Court

It must be noted at the outset that the question of the areas of competence of the European Union presents itself differently depending on whether the competence in issue has already been accorded to the European Union in the broad sense or has not yet been accorded to it. In the first hypothesis, it is a question of ruling on the division of areas of competence within the Union and, more particularly, on whether it is appropriate to proceed by way of a directive based on the EC Treaty or by way of a framework decision based on the EU Treaty. By contrast, in the second hypothesis, it is a question of ruling on the division of areas of competence between the Union and the Member States and, more particularly, on whether the Union has encroached on the latters' areas of competence. The present case comes under the first of those two hypotheses.

It must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24.

Ireland, supported by the Slovak Republic, contends that Directive 2006/24 cannot be based on Article 95 EC since its 'centre of gravity' does not concern the functioning of the internal market.

The sole objective of the directive, or at least its principal objective, is, it is contended, the investigation, detection and prosecution of crime.

That argument cannot be accepted.

According to the Court's settled case-law, the choice of legal basis for a Community measure must rest on objective factors which are amenable to judicial review, including in particular the aim and the content of the measure (see Case C-440/05 *Commission* v *Council* [2007] ECR I-9097, paragraph 61 and the case-law cited).

Directive 2006/24 was adopted on the basis of the EC Treaty and, in particular, Article 95 EC.

Article 95(1) EC provides that the Council is to adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

The Community legislature may have recourse to Article 95 EC in particular where disparities exist between national rules which are such as to obstruct the fundamental freedoms or to create distortions of competition and thus have a direct effect on the functioning of the internal market (see, to that effect, Case C-380/03 *Germany* v *Parliament and Council* [2006] ECR I-11573, paragraph 37 and the case-law cited).

Furthermore, although recourse to Article 95 EC as a legal basis is possible if the aim is to prevent the emergence of future obstacles to trade resulting from the divergent development of national laws, the emergence of such obstacles must be likely and the measure in question must be designed to prevent them (*Germany* v *Parliament and Council*, paragraph 38 and the case-law cited).

It is necessary to ascertain whether the situation which led to the adoption of Directive 2006/24 satisfies the conditions set out in the preceding two paragraphs.

As is apparent from recitals 5 and 6 in the preamble to that directive, the Community legislature started from the premiss that there were legislative and technical disparities between the national provisions governing the retention of data by service providers.

In that connection, the evidence submitted to the Court confirms that, following the terrorist attacks mentioned in paragraph 36 of this judgment, several Member States, realising that data relating to electronic communications constitute an effective means for the detection and prevention of crimes, including terrorism, adopted measures pursuant to Article 15(1) of Directive 2002/58 with a view to imposing obligations on service providers concerning the retention of such data.

It is also clear from the file that the obligations relating to data retention have significant economic implications for service providers in so far as they may involve substantial investment and operating costs.

The evidence submitted to the Court shows, moreover, that the national measures adopted up to 2005 pursuant to Article 15(1) of Directive 2002/58 differed substantially, particularly in respect of the nature of the data retained and the periods of data retention.

Finally, it was entirely foreseeable that the Member States which did not yet have rules on data retention would introduce rules in that area which were likely to accentuate even further the differences between the various existing national measures.

In the light of that evidence, it is apparent that the differences between the various national rules adopted on the retention of data relating to electronic communications were liable to have a direct impact on the functioning of the internal market and that it was foreseeable that that impact would become more serious with the passage of time.

Such a situation justified the Community legislature in pursuing the objective of safeguarding the proper functioning of the internal market through the adoption of harmonised rules.

Furthermore, it must also be noted that, by laying down a harmonised level of retention of data relating to electronic communications, Directive 2006/24 amended the provisions of Directive 2002/58.

Directive 2002/58 is based on Article 95 EC.

Under Article 47 EU, none of the provisions of the EC Treaty may be affected by a provision of the EU Treaty. That requirement appears in the first paragraph of Article 29 EU, which introduces Title VI of the EU Treaty, entitled 'Provisions on police and judicial cooperation in criminal matters' (Case C-440/05 *Commission* v *Council*, paragraph 52).

In providing that nothing in the EU Treaty is to affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them, Article 47 EU aims, in accordance with the fifth indent of Article 2 EU and the first paragraph of Article 3 EU, to maintain and build on the *acquis communautaire* (Case C-91/05 *Commission* v *Council* [2008] ECR I-0000, paragraph 59).

It is the task of the Court to ensure that acts which, according to one party, fall within the scope of Title VI of the Treaty on European Union and which, by their nature, are capable of having legal effects, do not encroach upon the powers conferred by the EC Treaty on the Community (Case C-91/05 *Commission* v *Council*, paragraph 33 and the case-law cited).

In so far as the amendment of Directive 2002/58 effected by Directive 2006/24 comes within the scope of Community powers, Directive 2006/24 could not be based on a provision of the EU Treaty without infringing Article 47 thereof.

In order to determine whether the legislature has chosen a suitable legal basis for the adoption of Directive 2006/24, it is also appropriate, as follows from paragraph 60 of this judgment, to examine the substantive content of its provisions.

In that connection, the provisions of Directive 2006/24 are essentially limited to the activities of service providers and do not govern access to data or the use thereof by the police or judicial authorities of the Member States.

More specifically, the provisions of Directive 2006/24 are designed to harmonise national laws on the obligation to retain data (Article 3), the categories of data to be retained (Article 5), the periods of retention of data (Article 6), data protection and data security (Article 7) and the conditions for data storage (Article 8).

By contrast, the measures provided for by Directive 2006/24 do not, in themselves, involve intervention by the police or law-enforcement authorities of the Member States. Thus, as is clear in particular from Article 3 of the directive, it is provided that service providers are to retain only data that are generated or processed in the course of the provision of the relevant communication services. Those data are solely those which are closely linked to the exercise of the commercial activity of the service providers.

Directive 2006/24 thus regulates operations which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonises neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities. Those matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the provisions of that directive, as is stated, in particular, in recital 25 in the preamble to, and Article 4 of, Directive 2006/24.

It follows that the substantive content of Directive 2006/24 is directed essentially at the activities of service providers in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty.

In light of that substantive content, Directive 2006/24 relates predominantly to the functioning of the internal market.

Against such a finding, Ireland argues that, by the judgment in *Parliament* v *Council and Commission*, the Court annulled Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, p. 83, and – corrigendum – OJ 2005 L 255, p. 168).

In paragraph 68 of the judgment in *Parliament* v *Council and Commission*, the Court held that that agreement related to the same transfer of data as did Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection (OJ 2004 L 235, p. 11).

The latter decision concerned the transfer of passenger data from the reservation systems of air carriers situated in the territory of the Member States to the United States Department of Homeland Security, Bureau of Customs and Border Protection. The Court held that that the subject-matter of that decision was data-processing which was not necessary for a supply of services by the air carriers, but which was regarded as necessary for safeguarding public security and for law-enforcement purposes. In paragraphs 57 to 59 of the judgment in *Parliament* v *Council and Commission*, the Court held that such data-processing was covered by Article 3(2) of Directive 95/46, according to which that directive does not apply, in particular, to the processing of personal data relating to public security and the activities of the State in areas of criminal law. The Court accordingly concluded that Decision 2004/535 did not fall within the scope of Directive 95/46.

Since the agreement which was the subject of Directive 2004/496 related, in the same way as Decision 2004/535, to data-processing which was excluded from the scope of Directive 95/46, the Court held that Decision 2004/496 could not have been validly adopted on the basis of Article 95 EC (*Parliament* v *Council and Commission*, paragraphs 68 and 69).

Such a line of argument cannot be transposed to Directive 2006/24.

Unlike Decision 2004/496, which concerned a transfer of personal data within a framework instituted by the public authorities in order to ensure public security, Directive 2006/24 covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law-enforcement purposes.

It follows that the arguments which Ireland draws from the annulment of Decision 2004/496 by the judgment in *Parliament* v *Council and Commission* cannot be accepted.

Having regard to all of the foregoing considerations, Directive 2006/24 had to be adopted on the basis of Article 95 EC.

The present action must accordingly be dismissed.

On those grounds, the Court (Grand Chamber) hereby:

1. **Dismisses the action;**

2. **Orders Ireland to pay the costs;**

3. **Orders the Kingdom of Spain, the Kingdom of the Netherlands, the Slovak Republic, the Commission of the European Communities and the European Data Protection Supervisor to bear their own respective costs.**

Related:

1. Opinion of Mr Advocate General Cruz Villalón delivered on 12 December 2013. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293
2. OPINION OF ADVOCATE GENERAL SAUGMANDSGAARD ØE delivered on 19 July 2016 (1) Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen (C-203/15) and Secretary of State for the Home Department

   http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=494057

Judgments of some national courts on data retention:

1. NÁLEZ Ústavního soudu 45/17

   https://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Publikovane_nalezy/2019/Pl._US_45_17_vcetne_disentu.pdf
2. Bundesverfassungsgericht. Urteil vom 2. März 2010. 1 BvR 256/08, 1 BvR 263/08 a 1 BvR 586/08.

   https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html
3. Wyrok Trybunalu Konstytucyjnego Sygn. akt K 23/11 z dnia 30 lipca 2014 r. *Trybunal Konstytucyjny*

   http://trybunal.gov.pl/postepowanie-i-orzeczenia/wyroki/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/
4. Belgium / Constitutional Court / 84/2015. 11 June 2015.

   https://fra.europa.eu/en/caselaw-reference/belgium-constitutional-court-842015
5. Slovenia / Constitutional Court / U-I-65/13-19. 3.7.2014.

   https://fra.europa.eu/en/caselaw-reference/slovenia-constitutional-court-u-i-6513-19
6. Nález Ústavného súdu Slovenskej republiky sp.zn. PL. ÚS 10/2014 ze 29. apríla 2015.

   https://www.ustavnysud.sk/ussr-intranet-portlet/docDownload/2fecbc69-fb5c-4ae8-92cf-1b0b5d9e4d3e/Rozhodnutie%20-%20N%C3%A1lez%20PL.%20%C3%9AS%2010_2014.pdf
7. Verfassungsgerichtshof. Urteil vom 27. Juni 2014. G-47/2012-49

   https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20140627_12G00047_00/JFT_20140627_12G00047_00.pdf

3. State of play in the member states - data retention

Working paper: Data Retention – State of play in the Member states

https://www.statewatch.org/news/2018/feb/eu-council-data-retention-state-of-play-ms-wk-5206-17.pdf

Member State	DR legislation in force	Status of the legislation	Relevant Court cases
Austria	No	Most parts of the Austrian law on data retention were declared invalid by the Constitutional Court on 27 June 2014 following the Ireland Digital Rights judgement of 8 March 2014. A legislative proposal is under preparation.	
Belgium	Yes	• **Law on the collection and retention of data in the telecommunications sector** (*Loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques*) The Law entered into force on 28 July 2016. • *Code d'instruction criminelle, articles 46bis et 88 bis* • *Loi du 30 novembre 1998 sur les services de renseignement de de sécurité, articles 13, 18 para 3 et 18, para 8* • *Loi du 13 juin 2005 relative aux communications électroniques, articles 126 suivants et 145*	
Bulgaria	Yes	• **Electronic Communications Act Prom. SG 41 of 22 May 2007**, last amended and supplemented by SG 103 of 27 December 2016 • Criminal Procedure Code Prom. SG 83 of 18 October 2005, last amended and	The previous Bulgarian data retention law was declared incompatible with the national constitution by the constitutional Court on 12 March 2015.

Member State	DR legislation in force	Status of the legislation	Relevant Court cases
		supplemented by SG. 13 of 7 February 2017	
Croatia	Yes	• **Electronic Communications Act**. • Criminal Procedure Act • Regulation on the obligations in the field of national security of the Republic of Croatia for legal and natural persons in telecommunications	
Cyprus	Yes	• **Law on the Retention of Telecommunications Data with a View to Investigating Serious Crimes** (183(i)/2008) as amended by Law 99(i)/2008	
Czech Republic	Yes	• **Electronic Communications Act** • Code of Criminal Procedure, Section 88a	
Denmark	Yes	• **Administration of Justice Act, Act no 1255** of 16 November 2015, Chapter 71 • Executive Order No. 988 of 28 September 2006 on the retention and storage of traffic data by providers of electronic communications networks and electronic communications services, amended by Executive Order no. 660 of 19 June 2014 (following the 2014 Digital Rights Ireland judgment) • Guidelines for the Executive Order on the retention and storage of traffic data by providers of electronic communications networks and electronic communications services	
Estonia	Yes	• **Electronic Communications Act**, based on Directive 2006/24/EC	

Member State	DR legislation in force	Status of the legislation	Relevant Court cases
Finland	Yes	• **Information Society Code 917/2014**, sections 157- 159 and 322 • The Act refers to the Police Act, the Border Guard Act (578/2005), the Act on the Processing of Personal Data by Border Guards (579/2005), the Customs Act (1466/1994) and the Coercive measures Act (806/2001)	
France	Yes	• **Post and Electronic Communications Law, in particular Article L34-1** (*Code des postes et des communications électroniques, notamment l'article L34-1).* • *Loi n 215-912 du 24 juillet 2015 relative au renseignement* • *Code de procédure pénale, articles 706-95-4 et 706-95-5* • *Loi n 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organise, le terrorisme et leur financement* • *Loi n 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et son décret d'application n 2011-2019 du 25 février 2011 relatif à la conservation et à la communication des données*	
Germany	Yes	• **Law on the introduction of an obligation to store and a maximum period to retain traffic data** (*Gesetz für Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*) The law entered into force on 18 December 2015, but the storage obligation becomes effective on 1 July 2017.	

Member State	DR legislation in force	Status of the legislation	Relevant Court cases
Greece	Yes	• **Act 3917/2011** (implementing Directive 2006/24)	
Hungary	Yes	• **2003 Electronic Communications Act** • Act XIX on Criminal Procedure of 1998 • Police Act XXXIV of 1995 • National Tax and Customs Office Act CXXII of 2010 • National Security Service Act CXXV of 1995 • Government decree 180/2004 (V.26) on electronic communications networks and bodies and agencies authorised to conduct covert investigations on cooperation between organisations	
Ireland	Yes	• **Communications (Retention of Data) Act 2011**	
Italy	Yes	• **Legislative Decree n. 109/2008** • **Legislative Decree n. 7 of 18 February 2015** (confirmed by law n. 43 of April 17, 2015)	
Latvia	Yes	• **Electronic Communications Act (Article 71)** • Criminal Procedure Act (Article 192) • Cabinet Regulation No 820 of 2007	
Lithuania	Yes	• **Electronic Communications Law No IX-2134 of 15 April 2004** (Articles 65, 66, 67 and 77) • Code of criminal Procedure (Article 154) • Law on Criminal Intelligence No XI-2234 of 2 October 2012 (Article 6)	
Luxembourg	Yes	• **Loi modifiée du 30 mai 2005**, relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des	

Member State	DR legislation in force	Status of the legislation	Relevant Court cases
		communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle	
Malta	Yes	• **Subsidiary Legislation 440.01 Processing of Personal Data (Electronic Communications Sector) Regulations of 15 July 2003 (last amended by Legal Notice 429 of 2013)**	
Netherlands	No	• The Data Retention Act of 1 September 2009 is no longer applicable following a ruling of the the Hague Civil Court of 15 March 2015 • Proposal of 13 September 2016 amending the Telecommunications Act and the Criminal Procedures Act in view of the retention of data processed in the context of providing public telecommunication services and public telecommunication networks (*Voorstel van wet van 13 september 2016 tot Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken*)	
Poland	Yes	• **Telecommunications law (**Dz. U. z 2016 r. poz. 1489)	
Portugal	Yes	• **Law No 32/2008 of 17 July transposing Directive 2006/24/EC**	
Romania	Yes	• **Law No 235/2015, amending Law No 506/2004, introducing rules regarding access of competent national authorities to retained data** (notably Articles 5 and 121)	The previous Romanian data retention law was declared unconstitutional by the Constitutional Court on 8 July 2014.

Member State	DR legislation in force	Status of the legislation	Relevant Court cases
		• Law No 75/2016, amending Law No 235/2015 and Government Emergency Order No 82/2014 (amending and supplementing Law No 135/2010 on the Code of Criminal Procedure (notably Articles 138 and 152).	
Slovakia	Yes	• **Act no. 351/2011 of 14 September 2014 on Electronic Communications**	
Slovenia	No	The Slovenian Constitutional Court annulled Chapter 13 on data retention of the Electronic Communications Act on 3 July 2014. No proposal has been made by the government to replace this law.	
Spain	Yes	• **Law 25/2007 of 18 October** on the retention of data concerning electronic communications and public communication networks, last amended on 10 May 2014 (*Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, consolidado de 10 de mayo de 2014*).	
Sweden	Yes	• **Law (2003:389) on electronic communications** *(Lagen (2003:389) om elektronisk kommunikation)* • Regulation (2003:396) on electronic communications (*Förordningen (2003:396) om elektronisk kommunikation*) • Law (2012:278) on gathering of data relating to electronic communications as part of intelligence gathering by law enforcement authorities (*Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i*	

Member State	DR legislation in force	Status of the legislation	Relevant Court cases
		de brottsbekämpande myndigheternas underrättelseverksamhet) • Code of Judicial Procedure (*Rättegångsbalken*)	
United Kingdom	Yes	• **Investigatory Powers Act 2016,** notably Part 3 on the Authorisations for obtaining communications data and Part 4 on the retention of communications data.	

4. New proposals on data retention

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=CS

1. CONTEXT OF THE PROPOSAL

1.1. Reasons for and objectives of the proposal

The Digital Single Market Strategy ("DSM Strategy") 1 has as an objective to increase trust in and the security of digital services. The reform of the data protection framework, and in particular the adoption of Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR") 2 , was a key action to this end. The DSM Strategy also announced the review of Directive 2002/58/EC ("ePrivacy Directive") 3 in order to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players. This proposal reviews the ePrivacy Directive, foreseeing in the DSM Strategy objectives and ensuring consistency with the GDPR.

The ePrivacy Directive ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector. It also guarantees the free movement of electronic communications data, equipment and services in the Union. It implements in the Union's secondary law the fundamental right to the respect for private life, with regard to communications, as enshrined in Article 7 of the Charter of Fundamental Rights of the European Union ("Charter").

In line with the 'Better Regulation' requirements, the Commission carried out an ex post Regulatory Fitness and Performance Programme ("REFIT evaluation") of the ePrivacy Directive. It follows from the evaluation that the objectives and principles of the current framework remain sound. However, important technological and economic developments took place in the market since the last revision of the ePrivacy Directive in 2009. Consumers and businesses increasingly rely on new internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and web-based e-mail services, instead of traditional communications services. These Over-the-Top communications services ("OTTs") are in general not subject to the current Union electronic communications framework, including the ePrivacy Directive. Accordingly, the Directive has not kept pace with technological developments, resulting in a void of protection of communications conveyed through new services.

Consistency with existing policy provisions in the policy area

This proposal is lex specialis to the GDPR and will particularise and complement it as regards electronic communications data that qualify as personal data. All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR. The alignment with the GDPR resulted in the repeal of some provisions, such as the security obligations of Article 4 of the ePrivacy Directive.

Consistency with other Union policies

The ePrivacy Directive is part of the regulatory framework for electronic communications. In 2016, the Commission adopted the proposal for a Directive establishing the European Electronic Communications Code ("EECC") 4 , which revises the framework. While the present proposal is not an integral part of the EECC, it partially relies on definitions provided therein, including that of 'electronic communications services'. Like the EECC, this proposal also brings OTT providers in

its scope to reflect the market reality. In addition, the EECC complements this proposal by ensuring the security of electronic communications services.

The Radio Equipment Directive 2014/53/EU ("RED") 5 ensures a single market for radio equipment. In particular, it requires that, before being placed on the market, radio equipment must incorporate safeguards to ensure that the personal data and privacy of the user are protected. Under the RED and the European Standardisation Regulation (EU) 1025/2012 6 , the Commission is empowered to adopt measures. This proposal does not affect the RED.

The proposal does not include any specific provisions in the field of data retention. It maintains the substance of Article 15 of the ePrivacy Directive and aligns it with specific wording of Article 23 of the GDPR, which provides grounds for Member States to restrict the scope of the rights and obligations in specific articles of the ePrivacy Directive. Therefore, Member States are free to keep or create national data retention frameworks that provide, inter alia, for targeted retention measures, in so far as such frameworks comply with Union law, taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights 7 .

Finally, the proposal does not apply to activities of Union institutions, bodies and agencies. However, its principles and relevant obligations as to the right to respect for private life and communications in relation to the processing of electronic communications data have been included in the Proposal for a Regulation repealing Regulation (EC) No 45/2001 8 .

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

2.1. Legal basis

Article 16 and Article 114 of the Treaty on the Functioning of the European Union ("TFEU") are the relevant legal bases for the proposal.

Article 16 TFEU introduces a specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, by Member States when carrying out activities falling within the scope of Union law, and rules relating to the free movement of such data. Since an electronic communication involving a natural person will normally qualify as personal data, the protection of natural persons with regard to the privacy of communications and processing of such data, should be based on Article 16.

In addition, the proposal aims at protecting communications and related legitimate interests of legal persons. The meaning and scope of the rights under Article 7 of the Charter shall, in accordance with Article 52(3) of the Charter, be the same as those laid down in Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"). As regards the scope of Article 7 of the Charter, the case-law of the Court of Justice of the European Union ("CJEU") 9 and of the European Court of Human Rights 10 confirm that professional activities of legal persons may not be excluded from the protection of the right guaranteed by Article 7 of the Charter and Article 8 of the ECHR.

Since the initiative pursues a twofold purpose and that the component concerning the protection of communications of legal persons and the aim of achieving the internal market for those electronic communications and ensure its functioning in this regard cannot be considered merely incidental, the initiative should, therefore, also be based on Article 114 of the TFEU.

2.2. Subsidiarity

Respect for communications is a fundamental right recognised in the Charter. Content of electronic communications may reveal highly sensitive information about the end-users involved in the communication. Similarly, metadata derived from electronic communications, may also reveal very sensitive and personal information, as expressely recognised by the CJEU 11 . The majority of Member States also recognise the need to protect communications as a distinct

constitutional right. Whilst it is possible for Member States to enact policies which ensure that this right is not breached, this would not be achieved in a uniform way in the absence of Union rules and would create restrictions on cross-border flows of personal and non-personal data related to the use of electronic communications services. Finally, to maintain consistency with the GDPR, it is necessary to review the ePrivacy Directive and adopt measures to bring the two instruments in line.

The technological developments and the ambitions of the DSM strategy have strengthened the case for action at the Union level. The success of the EU DSM depends on how effectively the EU brings down national silos and barriers and seize the advantages and economies of a European digital single market. Moreover, as internet and digital technologies know no borders, the dimension of the problem goes beyond the territory of a single Member State. Member States cannot effectively solve the problems in the current situation. A level playing field for economic operators providing substitutable services and equal protection of end-users at Union level are requirements for the DSM to work properly.

2.3. Proportionality

To ensure the effective legal protection of respect for privacy and communications, an extension of scope to cover OTT providers is necessary. While several popular OTT providers already comply, or partially comply with the principle of confidentiality of communications, the protection of fundamental rights cannot be left to self-regulation by industry. Also, the importance of the effective protection of privacy of terminal equipment is increasing as it has become indispensable in personal and professional life for the storage of sensitive information. The implementation of the ePrivacy Directive has not been effective to empower end-users. Therefore the implementation of the principle by centralising consent in software and prompting users with information about the privacy settings thereof, is necessary to achieve the aim. Regarding the enforcement of this Regulation, it relies on the supervisory authorities and the consistency mechanism of the GDPR. Moreover, the proposal allows Member States to take national derogatory measures for specific legitimate purposes. Thus, the proposal does not go beyond what is necessary to achieve the aims and complies with the principle of proportionality as set out in Article 5 of the Treaty on European Union. The obligations put on affected services are kept to a level as minimum as possible, while not impinging on the fundamental rights concerned.

2.4. Choice of the instrument

The Commission puts forward a proposal for a Regulation in order to ensure consistency with the GDPR and legal certainty for users and businesses alike by avoiding divergent interpretation in the Member States. A Regulation can ensure an equal level of protection throughout the Union for users and lower compliance costs for businesses operating across borders.

From the proposal:

Article 6 - Permitted processing of electronic communications data
2.Providers of electronic communications services may process electronic communications metadata if:

(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 28 for the duration necessary for that purpose; or

(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of

specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

Electronic evidence

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

Chapter 1: Subject matter, definitions and scope

Article 1. Subject matter

1. This Regulation lays down the rules under which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data. This Regulation is without prejudice to the powers of national authorities to compel service providers established or represented on their territory to comply with similar national measures.

2. This Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the TEU, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement or judicial authorities in this respect shall remain unaffected.

Article 2. *Definitions*

For the purpose of this Regulation, the following definitions shall apply:

1. 'European Production Order' means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence;

2. 'European Preservation Order' means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production;

3. 'service provider' means any natural or legal person that provides one or more of the following categories of services:

(a) electronic communications service as defined in Article 2(4) of [Directive establishing the European Electronic Communications Code];

(b) information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[333] for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers;

[333] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(c) internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrars and related privacy and proxy services;

4. 'offering services in the Union' means:

(a) enabling legal or natural persons in one or more Member State(s) to use the services listed under (3) above; and

(b) having a substantial connection to the Member State(s) referred to in point (a);

5. 'establishment' means either the actual pursuit of an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or a stable infrastructure from where the business is managed;

6. 'electronic evidence' means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data;

7. 'subscriber data' means any data pertaining to:

(a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email;

(b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;

8. 'access data' means data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];

9. 'transactional data' means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitues access data. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];

10. 'content data' means any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data;

11. 'information system' means information system as defined in point (a) of Article 2 of Directive 2013/40/EU of the European Parliament and of the Council[334];

12. 'issuing State' means the Member State in which the European Production Order or the European Preservation Order is issued;

---

[334] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

13. 'enforcing State' means the Member State in which the addressee of the European Production Order or the European Preservation Order resides or is established and to which the European Production Order and the European Production Order Certificate or the European Preservation Order and the European Preservation Order Certificate are transmitted for enforcement;

14. 'enforcing authority' means the competent authority in the enforcing State to which the European Production Order and the European Production Order Certificate or the European Preservation Order and the European Preservation Order Certificate are transmitted by the issuing authority for enforcement;

15. 'emergency cases' means situations where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC[335].

Article 3. ***Scope***
1. This Regulation applies to service providers which offer services in the Union.

2. The European Production Orders and European Production Orders may only be issued for criminal proceedings, both during the pre-trial and trial phase. The Orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or punished in the issuing State.

3. The Orders provided for by this Regulation may be issued only for data pertaining to services as defined in Article 2(3) offered in the Union.

Chapter 2: European Production Order, European Preservation Order and Certificates

Article 4 . Issuing authority
1. European Production Order for subscriber data and access data may be issued by:

(a) a judge, a court, an investigating judge or prosecutor competent in the case concerned; or

(b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court, an investigating judge or a prosecutor in the issuing State.

2. A European Production Order for transactional and content data may be issued only by:

(a) a judge, a court or an investigating judge competent in the case concerned; or

(b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court or an investigating judge in the issuing State.

[335] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 34523.12.2008. p 75).

3. A European Preservation Order may be issued by:

(a) a judge, a court, an investigating judge or prosecutor competent in the case concerned; or

(b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Preservation Order shall be validated, after examination of its conformity with the conditions for issuing a European Preservation Order under this Regulation, by a judge, a court, an investigating judge or a prosecutor in the issuing State.

4. Where the Order has been validated by a judicial authority pursuant to paragraphs 1(b), 2(b) and 3(b), that authority may also be regarded as an issuing authority for the purposes of transmission of the European Production Order Certificate and the European Preservation Order Certificate.

Article 5. Conditions for issuing a European Production Order

1. An issuing authority may only issue a European Production Order where the conditions set out in this Article are fulfilled.

2. The European Production Order shall be necessary and proportionate for the purpose of the proceedings referred to in Article 3 (2) and may only be issued if a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State.

3. European Production Orders to produce subscriber data or access data may be issued for all criminal offences.

4. European Production Orders to produce transactional data or content data may only be issued

(a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or

(b) for the following offences, if they are wholly or partly committed by means of an information system:

– offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA[336];

– offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council[337];

– offences as defined in Articles 3 to 8 of Directive 2013/40/EU, of the European Parliament and of the Council;

(c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council[338].

5. The European Production Order shall include the following information:

(a) the issuing and, where applicable, the validating authority;

(b) the addressee of the European Production Order as referred to in Article 7;

---

[336] Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (OJ L 149, 2.6.2001, p. 1).
[337] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).
[338] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

(c) the persons whose data is being requested, except where the sole purpose of the order is to identify a person;

(d) the requested data category (subscriber data, access data, transactional data or content data);

(e) if applicable, the time range requested to be produced;

(f) the applicable provisions of the criminal law of the issuing State;

(g) in case of emergency or request for earlier disclosure, the reasons for it;

(h) in cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, a confirmation that the Order is made in accordance with paragraph 6;

(i) the grounds for the necessity and proportionality of the measure.

6. In cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the European Production Order may only be addressed to the service provider where investigatory measures addressed to the company or the entity are not appropriate, in particular because they might jeopardise the investigation.

7. If the issuing authority has reasons to believe that, transactional or content data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed, or its disclosure may impact fundamental interests of that Member State such as national security and defence, the issuing authority has to seek clarification before issuing the European Production Order, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network. If the issuing authority finds that the requested access, transactional or content data is protected by such immunities and privileges or its disclosure would impact fundamental interests of the other Member State, it shall not issue the European Production Order.

Article 6. Conditions for issuing a European Preservation Order

1. An issuing authority may only issue a European Preservation Order where the conditions set out in this Article are fulfilled.

2. It may be issued where necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via mutual legal assistance, a European Investigation Order or a European Production Order. European Preservation Orders to preserve data may be issued for all criminal offences.

3. The European Preservation Order shall include the following information:

(a) the issuing and, where applicable, the validating authority;

(b) the addressee of the European Preservation Order as referred to in Article 7;

(c) the persons whose data shall be preserved, except where the sole purpose of the order is to identify a person;

(d) the data category to be preserved (subscriber data, access data, transactional data or content data);

(e) if applicable, the time range requested to be preserved;

(f) the applicable provisions of the criminal law of the issuing State;

(g) the grounds for the necessity and proportionality of the measure.

Article 7. Addressee of a European Production Order and a European Preservation Order

1. The European Production Order and the European Preservation Order shall be addressed directly to a legal representative designated by the service provider for the purpose of gathering evidence in criminal proceedings.

2. If no dedicated legal representative has been appointed, the European Production Order and the European Preservation Order may be addressed to any establishment of the service provider in the Union.

3. Where the legal representative does not comply with an EPOC in an emergency case pursuant to Article 9(2), the EPOC may be addressed to any establishment of the service provider in the Union.

4. Where the legal representative does not comply with its obligations under Articles 9 or 10 and the issuing authority considers that there is a serious risk of loss of data, the European Production Order or the European Preservation Order may be addressed to any establishment of the service provider in the Union.

Article 8. European Production and Preservation Order Certificate

1. A European Production or Preservation Order shall be transmitted to the addressee as defined in Article 7 through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).

The issuing or validating authority shall complete the EPOC set out in Annex I or the EPOC-PR set out in Annex II, shall sign it and shall certify its content as being accurate and correct.

2. The EPOC or the EPOC-PR shall be directly transmitted by any means capable of producing a written record under conditions allowing the addressee to establish its authenticity.

Where service providers, Member States or Union bodies have established dedicated platforms or other secure channels for the handling of requests for data by law enforcement and judicial authorities, the issuing authority may also choose to transmit the Certificate via these channels.

3. The EPOC shall contain the information listed in Article 5(5) (a) to (h), including sufficient information to allow the addressee to identify and contact the issuing authority. The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included.

4. The EPOC-PR shall contain the information listed in Article 6(3) (a) to (f), including sufficient information to allow the addressee to identify and contact the issuing authority. The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included.

5. Where needed, the EPOC or the EPOC-PR shall be translated into an official language of the Union accepted by the addressee. Where no language has been specified, the EPOC or the EPOC-PR shall be translated into one of the official languages of the Member State where the legal representative resides or is established.

Article 9. Execution of an EPOC

1. Upon receipt of the EPOC, the addressee shall ensure that the requested data is transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the latest within 10 days upon receipt of the EPOC, unless the issuing authority indicates reasons for earlier disclosure.

2. In emergency cases the addressee shall transmit the requested data without undue delay, at the latest within 6 hours upon receipt of the EPOC.

3. If the addressee cannot comply with its obligation because the EPOC is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC, the addressee shall inform the issuing authority referred to in the EPOC without undue delay and ask for clarification, using the Form set out in Annex III. It shall inform the issuing authority whether an identification and preservation was possible as set out in paragraph 6. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1 and 2 shall not apply until the clarification is provided.

4. If the addressee cannot comply with its obligation because of *force majeure* or of de facto impossibility not attributable to the addressee or, if different, the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC, the addressee shall inform the issuing authority referred to in the EPOC without undue delay explaining the reasons, using the Form set out in Annex III. If the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC.

5. In all cases where the addressee does not provide the requested information, does not provide it exhaustively or does not provide it within the deadline, for other reasons, it shall inform the issuing authority without undue delay and at the latest within the deadlines set out in paragraphs 1 and 2 of the reasons for this using the Form in Annex III. The issuing authority shall review the order in light of the information provided by the service provider and if necessary, set a new deadline for the service provider to produce the data.

In case the addressee considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive, the addressee shall also send the Form in Annex III to the competent enforcement authority in the Member State of the addressee. In such cases the competent enforcement authority may seek clarifications from the issuing authority on the European Production Order, either directly or via Eurojust or the European Judicial Network.

6. The addressee shall preserve the data requested, if it does not produce it immediately, unless the information in the EPOC does not allow it to identify the data requested, in which case it shall seek clarification in accordance with paragraph 3. The preservation shall be upheld until the data is produced, whether it is on the basis of the clarified European Production Order and its Certificate or through other channels, such as mutual legal assistance. If the production of data and its preservation is no longer necessary, the issuing authority and where applicable pursuant to Article 14(8) the enforcing authority shall inform the addressee without undue delay.

Article 10. Execution of an EPOC-PR

1. Upon receipt of the EPOC-PR, the addressee shall, without undue delay, preserve the data requested. The preservation shall cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been launched.

2. If the issuing authority confirms within the time period set out in paragraph 1 that the subsequent request for production has been launched, the addressee shall preserve the data as long as necessary to produce the data once the subsequent request for production is served.

3. If the preservation is no longer necessary, the issuing authority shall inform the addressee without undue delay.

4. If the addressee cannot comply with its obligation because the Certificate is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC-PR, the addressee shall inform the issuing authority set out in the EPOC-PR without undue delay and ask for clarification, using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The addressee shall ensure that on its side the needed clarification can be received in order to fulfil its obligation set out in paragraph 1.

5. If the addressee cannot comply with its obligation because of *force majeure,* or of de facto impossibility not attributable to the addressee or, if different, the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the Order, it shall contact the issuing authority set out in the EPOC-PR without undue delay explaining the reasons, using the Form set out in Annex III. If these conditions are fulfilled, the issuing authority shall withdraw the EPOC-PR.

6. In all cases where the addressee does not preserve the requested information, for other reasons listed in the Form of Annex III, the addressee shall inform the issuing authority without undue delay of the reasons for this in the Form set out in Annex III. The issuing authority shall review the Order in light of the justification provided by the service provider.

Article 11. Confidentiality and user information
1. Addressees and, if different, service providers shall take the necessary measures to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved and where requested by the issuing authority, shall refrain from informing the person whose data is being sought in order not to obstruct the relevant criminal proceedings.

2. Where the issuing authority requested the addressee to refrain from informing the person whose data is being sought, the issuing authority shall inform the person whose data is being sought by the EPOC without undue delay about the data production. This information may be delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings.

3. When informing the person, the issuing authority shall include information about any available remedies as referred to in Article 17.

Article 12. Reimbursement of costs
The service provider may claim reimbursement of their costs by the issuing State, if this is provided by the national law of the issuing State for domestic orders in similar situations, in accordance with these national provisions.

Chapter 3: Sanctions and enforcement

Article 13. *Sanctions*
Without prejudice to national laws which provide for the imposition of criminal sanctions, Member States shall lay down the rules on pecuniary sanctions applicable to infringements of the obligations pursuant to Articles 9, 10 and 11 of this Regulation and shall take all necessary measures to ensure that they are implemented. The pecuniary sanctions provided for shall be effective, proportionate and dissuasive. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

Article 14. Procedure for enforcement
1. If the addressee does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons accepted by the issuing authority, the issuing authority may transfer to the competent authority in the enforcing State the European Production Order with the EPOC or the European Preservation Order with the EPOC-PR as well as the Form set out in Annex III filled out by the addressee and any other relevant document with a view to its enforcement by any means capable of producing a written record under conditions allowing the enforcing authority to establish authenticity. To this end, the issuing authority shall translate the Order, the Form and any other accompanying documents into one of the official languages of this Member State and shall inform the addressee of the transfer.

2. Upon receipt, the enforcing authority shall without further formalities recognise a European Production Order or European Preservation Order transmitted in accordance with paragraph 1 and shall take the necessary measures for its enforcement, unless the enforcing authority considers that one of the grounds provided for in paragraphs 4 or 5 apply or that the data concerned is protected by an immunity or privilege under its national law or its disclosure may impact its fundamental interests such as national security and defence. The enforcing authority shall take the decision to recognise the Order without undue delay and no later than 5 working days after the receipt of the Order.

3. Where the enforcing authority recognises the Order, it shall formally require the addressee to comply with the relevant obligation, informing the addressee of the possibility to oppose the enforcement by invoking the grounds listed in paragraphs 4 or 5, as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition.

4. The addressee may only oppose the enforcement of the European Production Order on the basis of the following grounds:

(a) the European Production Order has not been issued or validated by an issuing authority as provided for in Article 4;

(b) the European Production Order has not been issued for an offence provided for by Article 5(4);

(c) the addressee could not comply with the EPOC because of de facto impossibility or force majeure, or because the EPOC contains manifest errors;

(d) the European Production Order does not concern data stored by or on behalf of the service provider at the time of receipt of EPOC;

(e) the service is not covered by this Regulation;

(f) based on the sole information contained in the EPOC, it is apparent that it manifestly violates the Charter or that it is manifestly abusive.

5. The addressee may only oppose the enforcement of the European Preservation Order on the basis of the following grounds:

(a) the European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4;

(b) the service provider could not comply with the EPOC-PR because of de facto impossibility or force majeure, or because the EPOC-PR contains manifest errors;

(c) the European Preservation Order does not concern data stored by or on behalf of the service provider at the time of the EPOC-PR;

(d) the service is not covered by the scope of the present Regulation;

(e) based on the sole information contained in the EPOC-PR, it is apparent that the EPOC-PR manifestly violates the Charter or is manifestly abusive.

6. In case of an objection by the addressee, the enforcing authority shall decide whether to enforce the Order on the basis of the information provided by the addressee and, if necessary, supplementary information obtained from the issuing authority in accordance with paragraph 7.

7. Before deciding not to recognise or enforce the Order in accordance with paragraph 2 and 6, the enforcing authority shall consult the issuing authority by any appropriate means. Where appropriate, it shall request further information from the issuing authority. The issuing authority shall reply to any such request within 5 working days.

8. All decisions shall be notified immediately to the issuing authority and to the addressee by any means capable of producing a written record.

9. If the enforcing authority obtains the data from the addressee, it shall transmit it to the issuing authority within 2 working days, unless the data concerned is protected by an immunity or privilege under its own domestic law or it impacts its fundamental interests such as national security and defence. In such case, it shall inform the issuing authority of the reasons for not transmitting the data.

10. In case the addressee does not comply with its obligations under a recognised Order whose enforceability has been confirmed by the enforcing authority, that authority shall impose a pecuniary sanction in accordance with its national law. An effective judicial remedy shall be available against the decision to impose a fine.

Chapter 4: Remedies

Article 15. Review procedure in case of conflicting obligations based on fundamental rights or fundamental interests of a third country

1. If the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country prohibiting disclosure of the data concerned on the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence, it shall inform the issuing authority of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5).

2. The reasoned objection shall include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country.

3. The issuing authority shall review the European Production Order on the basis of the reasoned objection. If the issuing authority intends to uphold the European Production Order, it shall request a review by the competent court in its Member State. The execution of the Order shall be suspended pending completion of the review procedure.

The competent court shall first assess whether a conflict exists, based on an examination of whether

(a) the third country law applies based on the specific circumstances of the case in question and if so,

(b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.

4. In carrying out this assessment, the court should take into account whether the third country law, rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence, manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations.

5. If the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. If the competent court establishes that a relevant conflict within the meaning of paragraphs 1 and 4 exists, the competent court shall transmit all relevant factual and legal information as regards the case, including its assessment, to the central authorities in the third country concerned, via its national central authority, with a 15 day deadline to respond.

Upon reasoned request from the third country central authority, the deadline may be extended by 30 days.

6. If the third country central authority, within the deadline, informs the competent court that it objects to the execution of the European Production Order in this case, the competent court shall lift the Order and inform the issuing authority and the addressee. If no objection is received within the (extended) deadline, the competent court shall send a reminder giving the third country central authority 5 more days to respond and informing it of the consequences of not providing a response. If no objection is received within this additional deadline, the competent court shall uphold the Order.

7. If the competent court determines that the Order is to be upheld, it shall inform the issuing authority and the addressee, who shall proceed with the execution of the Order.

Article 16. Review procedure in case of conflicting obligations based on other grounds

1. If the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country prohibiting disclosure of the data concerned on other grounds than those referred to in Article 15, it shall inform the issuing authority of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5).

2. The reasoned objection must include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country.

3. The issuing authority shall review the European Production Order on the basis of the reasoned objection. If the issuing authority intends to uphold the European Production Order, it shall request a review by the competent court in its Member State. The execution of the Order shall be suspended pending completion of the review procedure.

4. The competent court shall first assess whether a conflict exists, based on an examination of whether

(a) the third country law applies based on the specific circumstances of the case in question and if so,

(b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.

5. If the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. If the competent court establishes that the third country law, when applied to the specific circumstances of the case under examination, prohibits disclosure of the data concerned, the competent court shall determine whether to uphold or withdraw the Order in particular on the basis of the following factors:

(a) the interest protected by the relevant law of the third country, including the third country's interest in preventing disclosure of the data;

(b) the degree of connection of the criminal case for which the Order was issued to either of the two jurisdictions, as indicated *inter alia* by:

the location, nationality and residence of the person whose data is being sought and/or of the victim(s),

the place where the criminal offence in question was committed;

(c) the degree of connection between the service provider and the third country in question; in this context, the data storage location by itself does not suffice in establishing a substantial degree of connection;

(d) the interests of the investigating State in obtaining the evidence concerned, based on the seriousness of the offence and the importance of obtaining evidence in an expeditious manner;

(e) the possible consequences for the addressee or the service provider of complying with the European Production Order, including the sanctions that may be incurred.

6. If the competent court decides to lift the Order, it shall inform the issuing authority and the addressee. . If the competent court determines that the Order is to be upheld, it shall inform the issuing authority and the addressee, who shall proceed with the execution of the Order.

Article 17. Effective remedies
1. Suspects and accused persons whose data was obtained via a European Production Order shall have the right to effective remedies against the European Production Order during the criminal proceedings for which the Order was issued, without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.

2. Where the person whose data was obtained is not a suspect or accused person in criminal proceedings for which the Order was issued, this person shall have the right to effective remedies against a European Production Order in the issuing State, without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.

3. Such right to an effective remedy shall be exercised before a court in the issuing State in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality.

4. Without prejudice to Article 11, the issuing authority shall take the appropriate measures to ensure that information is provided about the possibilities under national law for seeking remedies and ensure that they can be exercised effectively.

5. The same time-limits or other conditions for seeking a remedy in similar domestic cases shall apply here and in a way that guarantees effective exercise of these remedies for the persons concerned.

6. Without prejudice to national procedural rules, Member States shall ensure that in criminal proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the European Production Order.

Article 18. Ensuring privileges and immunities under the law of the enforcing State
If transactional or content data obtained by the European Production Order is protected by immunities or privileges granted under the law of the Member State of the addressee, or it impacts fundamental interests of that Member State such as national security and defence, the court in the issuing State shall ensure during the criminal proceedings for which the Order was issued that these grounds are taken into account in the same way as if they were provided for under their national law when assessing the relevance and admissibility of the evidence concerned. The court may consult the authorities of the relevant Member State, the European Judicial Network in criminal matters or Eurojust.

Chapter 5: Final provisions

Article 19. Monitoring and reporting
1. By *[date of application of this Regulation]* at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the means by which and the intervals at which the data and other

necessary evidence will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence.

2. In any event, Member States shall collect and maintain comprehensive statistics from the relevant authorities. The data collected shall be sent to the Commission each year by 31 March for the preceding calendar year and shall include:

(a) the number of EPOCs and EPOC-PRs issued by type of data requested, service providers addressed and situation (emergency case or not);

(b) the number of fulfilled and non-fulfilled EPOCs by type of data requested, service providers addressed and situation (emergency case or not);

(c) for fulfilled EPOCs, the average duration for obtaining the requested data from the moment the EPOC is issued to the moment it is obtained, by type of data requested, service provider addressed and situation (emergency case or not);

(d) the number of European Production Orders transmitted and received for enforcement to an enforcing State by type of data requested, service providers addressed and situation (emergency case or not) and the number thereof fulfilled;

(e) the number of legal remedies against European Production Orders in the issuing State and in the enforcing State by type of data requested.

Article 20. Amendments to the Certificates and the Forms
The Commission shall adopt delegated acts in accordance with Article 21 to amend Annexes I, II and III in order to effectively address a possible need for improvements regarding the content of EPOC and EPOC-PR forms and of forms to be used to provide information on the impossibility to execute the EPOC or EPOC-PR.

Article 21. Exercise of delegation
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 20 shall be conferred for an indeterminate period of time from *[date of application of this Regulation]*.

3. The delegation of powers referred to in Article 20 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[339].

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 20 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they

[339] OJ L 123, 12.5.2016, p. 13.

will not object. That period shall be extended by 2 months at the initiative of the European Parliament or of the Council.

Article 22. Notifications
1. By *[date of application of this Regulation]* each Member State shall notify the Commission of the following:

(a) the authorities which, in accordance with its national law, are competent in accordance with to Article 4 to issue and/or validate European Production Orders and European Preservation Orders;

(b) the enforcing authority or authorities which are competent to enforce European Production Orders and European Preservation Orders on behalf of another Member State;

(c) the courts competent to deal with reasoned objections by addressees in accordance with Articles 15 and 16.

2. The Commission shall make the information received under this Article publicly available, either on a dedicated website or on the website of the European Judicial Network referred to in Article 9 of the Council Decision 2008/976/JHA[340].

Article 23. Relationship to European Investigation Orders
Member States' authorities may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU for the gathering of evidence that would also fall within the scope of this Regulation.

Article 24. *Evaluation*
By *[5 years from the date of application of this Regulation]* at the latest, the Commission shall carry out an evaluation of the Regulation and present a report to the European Parliament and to the Council on the functioning of this Regulation, which shall include an assessment of the need to enlarge its scope. If necessary, the report shall be accompanied by legislative proposals. The evaluation shall be conducted according to the Commission's better regulation guidelines. Member States shall provide the Commission with the information necessary for te preparation of that Report.

Article 25. Entry into force
This Regulation shall enter into force on the twentieth day following its publication in the *Official Journal of the European Union*.

It shall apply from *[6 months after its entry into force]*.

[340] Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).

CYBERSECURITY LAW CASEBOOK 2020

Anna-Maria Osula, Bríd Ní Ghráinne, Dan Svantesson, David Kosař, Don Ferguson, Ivana Kudláčková, Jakub Klodwig, Jakub Vostoupal, Kateřina Uhlířová, Jan Kolouch, Veronika Žolnerčíková

Published by Masaryk University
Žerotínovo nám. 617/9, 601 77 Brno, Czech Republic
in 2021

Publications of the Masaryk University No. 706
(theoretical series, edition Scientia)

1st edition, 2021

ISBN 978-80-210-9774-2 (online ; pdf)
www.law.muni.cz