NIS Directive

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

A Commentary
(excerpts)

Sandra Schmitz-Berndt and Mark D. Cole

Luxembourg
National
Research Fund

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

—A Commentary (excerpts)—

Sandra Schmitz-Berndt and Mark D. Cole

Last update: September 2023

Today's economy, and by this, citizens of the EU, depend on reliable network and information services. Despite a wide selection of technical protection measures being available, attacks on network and information systems (NIS) are on the rise in number and impact. The EU's Cybersecurity Strategy includes the NIS Directive, a legal instrument designed to ensure that critical IT systems in central sectors of the economy are secure. Analyzing how the legal requirements under this new framework align with software requirements, and vice versa, necessitates a collaborative effort between legal and technical experts.

Against this background, the FNR-funded EnCaViBS project (Enhancing Cybersecurity across Vital Business Sectors) aimed to clarify the abstract legal concepts and notions of the NIS Directive to facilitate the development of compliant products. Guidance was to be provided by a living online article-by-article commentary on the NIS Directive, which examines each article of the NIS Directive in sequential order and explains how the

provisions work and have been transposed and interpreted by national legislators. This working paper includes excerpts from the living commentary compiled during the project run-time, reflecting its latest update as of September 2023. In view of the NIS Directive being repealed and replaced by the NIS 2 Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80) adopted in December 2022, the commentary also addresses the deficiencies and deficits of the NIS Directive identified during its review and how the NIS 2 Directive seeks to respond to these issues.
The content is also accessible via http://encavibs.daloos.uni.lu/neu-NIS Directive-commentary/

The excerpts have been authored by Sandra Schmitz-Berndt and Mark D. Cole, except for the comment on Article 21 NIS Directive, which has been provided by Paula Contreras. The authors would like to thank Paula for her contribution.

Acknowledgement: The research for this contribution was funded by the Luxembourg National Research Fund (FNR)C18/IS/12639666/EnCaViBS/Cole (https://www.fnr.lu/projects/the-eu-nisdirective-enhancingcybersecurity-across-vital-business-sectors-encavibs/).

Inhalt

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 Article19 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.

I. General Remarks

Article 1 outlines the general subject matter and scope of the NIS Directive.

II. In Detail

Article 1(1) Scope and General Aim

Article 1(1) NIS Directive presents the scope and general aim of the Directive, namely the implementation of measures to achieve a high common level of security of network and information systems within the EU so as to improve the functioning of the internal market. The market rationale refers to Article 114 TFEU as the legislative basis for regulating the security of network and information systems.

Article 1(2) Main Measures

Article 1(2) NIS Directive outlines the main measures to achieve the envisaged high common level of security of network and information systems within the Union set out in Article 1(1).

Pursuant to Article 1(2)(a) NIS Directive, Member States must adopt a national strategy on the security of network and information systems, which, defines the strategic objectives and concrete policy actions to be implemented. Article 4(3) NIS Directive defines 'national strategy on the security of network and information systems' as a framework providing strategic objectives and priorities on the security of network and information systems at national level. Article 7 then specifies the content of such a national strategy.

Although one may argue, that the subject matter of cybersecurity is not identical with NIS security, Member States commonly employ the notion of cybersecurity strategy rather than national NIS strategy (for instance Luxembourg). An overview of national cybersecurity strategies (NCSS) is provided by the European Union Agency for Cybersecurity (ENISA) in an interactive map. The interactive map also provides access to English translations of most strategies.

ENISA has been supporting EU Member States to develop, implement and update national cybersecurity strategies since publishing its first National Cyber Security Strategy Good Practice Guide in 2012.

In the following, Article 1(2)(b) NIS Directive foresees as a second measure to achieve the aims of the Directive, the creation of a Cooperation Group (NIS CG). The composition and tasks of this group are further detailed in Article 11: the NIS CG is composed of representatives of Member States, the Commission, and ENISA. The role of the NIS CG is to support, assist Member States when applying the Directive and serve as an instrument for the exchange of best practice, discussion of capabilities and preparedness of the Member States. The NIS CG for instance shall support Member States in taking a consistent approach in the process of identification of operators of essential services (OES) (Article 5(6)). The NIS CG's role is set at a policy level, and thus, instructions are not binding. The respective tasks of the NIS CG and of ENISA are interdependent and complementary (Recital 38). The NIS CG also cooperates with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practice, and to provide advice on security aspects of NIS that might have an impact on their work (Recital 38 NIS Directive). For more information on the NIS CG see comment on Article 11 NIS Directive.

Article 1(2)(c) NIS Directive sets out the third measure to achieve the aims of the Directive, namely the creation of a Computer Incident Response Teams (CSIRTs) network composed of representatives of the Member States' national CSIRTs and CERT-EU (see Article 12). The CSIRTs network serves as a platform for cooperation and information exchange. The idea is to improve the handling of cross-border incidents and allow for coordinated responses. For more information on the CSIRTs network see comment on Article 12 NIS Directive.

Article 1(2)(d) NIS Directive addresses a fourth measure to achieve the aims of the Directive: the obligation of Member States to implement security and notification requirements for OES and digital services providers (DSP). The minimum requirements are set out in Article 14 NIS Directive (as regards OES) and Article 16 NIS Directive (as regards DSP).

A fifth measure to achieve the aims of the Directive is set out in Article 1(2)(e) NIS Directive and addresses the designation of national competent authorities (NCAs), single points of contact (SPOCs) and CSIRTs. The Directive recognises that in view of the differences in national governance structures (e.g. sectoral regulatory arrangements), Member States may designate more than one national competent authority for fulfilling the tasks linked to the security of NIS under the Directive (Recital 30 NIS Directive). The designation of a national single point of contact however is consider as a necessity to actually facilitate cross-border cooperation and communication.

Article 1(3) Exemptions to the Scope of Application

Exemptions to the scope of application are stipulated in Article 1(3) NIS Directive relating to the telecoms sector and trust service providers which are subject to the requirements of Article 19 eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and

of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73). Article 1(3) NIS Directive excludes undertakings providing public communications networks or publicly available electronic communications services, which are subject to the requirements of Articles 13a and 13b Framework Directive (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 [2002] OJ L108/33) from the security and notification requirements of the NIS Directive. This was due to the fact, that Article 13a Framework Directive provided similar obligations. Although the Framework Directive has been repealed by the Electronic Communications Code (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (EECC) [2018] OJ L321/36), providers of public electronic communications networks or of publicly available electronic communications services continue to be exempted from the security and notification requirements of the NIS Directive because Article 40 EECC provides for similar requirements. However, in practice, this means that undertakings providing services within the definition of Article 2(a) Framework Directive may be identified as OES or DSP (now Article 2(8) EECC), but only have to comply with the obligations of the NIS Directive for services they provide that are distinct from the provision of public communications networks or electronic communications services (as sector-specific legislation in that regard exists). The services under the scope of the NIS Directive are those referred to in Annex II.

Article 1(4) Effect on the Application of ECI Directive, the Directive on Combating Child Sexual Abuse and the Directive on Attacks against Information Systems

The NIS Directive does not affect the application of the ECI Directive (Council Directive 2008/114/EC of 8 December 2008 on identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75), the Directive on combating child sexual abuse (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 [2011] OJ L335/1) and the Directive on attacks against information systems (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 [2013] OJ L218/8).

Article 1(5) Ensuring Confidentiality

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 (cf. Recital 41 NIS Directive).

Article 1(6) Safeguarding Essential State Functions

In consideration of the interests of Member States, safeguarding essential state functions precedes.

Article 1(7) Relationship between the NIS Directive and Sector-Specific EU Legislation

Article1(7) NIS Directive regulates the interface between the NIS Directive and other sector-specific EU legislation. It recognises that 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 NIS. In other words, pre-existing and future sector- or topic-specific legislation shall retain primary applicability in the sense of lex specialis, so that at least in principle contradictions between overlapping requirements can be avoided.

Whenever sector-specific 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 (Recital 9). Noteworthy, Article1(7) only requires that the Union legal act requires the implementation of network and information systems security or the notification of incidents with equivalent effect. It is thus unclear, whether an obligation to ensure the security of NIS laid down in a sector-specific Union legal act will suffice for the sector-specific act to gain precedence (cf. Charlotte Ducuing, 'On the Edge of the NIS Directive: The Proposed C-ITS Delegated Regulation, Friend or Foe?' [2019] CiTiP Working Paper). In contrast to Article1(7), Recital 9 refers to the implementation of security measures and notification of incidents.

In determining whether the requirements on the security and the notification of incidents contained in sector-specific Union legal acts are equivalent to those contained in this Directive, regard should only be paid to the provisions of relevant Union legal acts and their application in the Member States (Recital 9).

In resolving the conflict or assessing the equivalent effect, the nature of the NIS Directive has to be born in mind. The NIS Directive as a Directive requires implementation into national law at Member State level; thus, any conflict with another Directive would occur at Member State level. In that line assessing the equivalent effect of a Regulation with the NIS Directive means in any case that the Regulation would prevail by its nature over Member State law (cf. with regard to the relationship between the NIS Directive and the GDPR: Dimitra Markopoulou, Vagelis Papakonstantinou & Paul de Hert, 'The new EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 105336).

If equivalent effect can be established, Member States should apply the provisions of the sector-specific Union legal act, including those relating to jurisdiction. In addition, they should not carry out the identification process for operators of essential services as defined

by the NIS Directive (Recital 9). Recital 9 clarifies that in this case, the Member State should provide information to the Commission on the application of such lex specialis provisions.

Equivalent effect has so far been established at EU level between Articles 95 and 96 PSD2 (Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35) relating to payment service providers and Article 14 NIS Directive (See European Commission, '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/2017/0476 final, Annex I, p. 37). Payment service providers are encompassed within Annex II of the NIS Directive as part of the financial services sector. Articles 95 and 96 PSD2 are lex specialis to the NIS Directive.

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.

I. General Remarks

Article 2 NIS Directive sets forth that the processing of personal data pursuant to the NIS Directive is in accordance with EU data protection legislation, referring to the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31) 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 ([2001] OJ L008/1).

II. In Detail

Article 2(1) Processing of Personal Data in Accordance with GDPR

1. Introductory Remarks

The Data Protection Directive sought to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States. It has been repealed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) ([2016] OJ L119/1) with effect from 25 May 2018. According to Article 94(2) GDPR, references to the repealed Directive are construed as references to the GDPR. In response to the differences in the level of protection of the rights and freedoms of natural persons under the Directive, the GDPR seeks to achieve a level of protection equivalent in all Member States.

2. The Relationship between the NIS Directive and the GDPR

Similar to the NIS Directive, the GDPR supports the EU Digital Single Market and protects the interests of European residents and the functioning of essential services in the EU. However, the NIS Directive and the GDPR have distinct interests. i.e. privacy of personal data as regards the GDPR and confidentiality of services as regards the NIS Directive. The relationship between the NIS Directive and the GDPR is not specifically addressed in either of the instruments. Whereas for instance the proposal for a new e-Privacy Regulation (European Commission, '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' COM(2017) 10 final) stipulates in Article 1(3) that its provisions particularise and complement the GDPR by laying down specific rules for the purposes mentioned in Article 1(1) and 1(2) of the Proposal, the NIS Directive contains a few general references to data protection provisions that do not specify the relationship of the instruments. Recital 63 NIS Directive acknowledges that competent authorities and data protection authorities (DPAs) should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from an incident. Recital 72 and Article 2 NIS Directive emphasize that if personal data is processed, such processing should comply with the Data Protection Directive and the EU Institutions Data Protection Regulation.

Article 94(2) GDPR sets forth that references to the repealed Directive shall be construed as references to the GDPR. In the following, Articles 8(6) and 15(4) NIS Directive require the competent authorities and single points of contact (SPOCs) under the NIS Directive to consult and cooperate with national DPAs. There is no further framework or guidance on such cooperation.

In this respect, several questions arise, for instance, whether the NIS Directive will create additional liability in cases where an operator has violated provisions of both laws, or whether compliance with the GDPR may serve as a defence to enforcement under the NIS Directive. There is a risk of double jeopardy for failure to comply with notification obligations or security requirements (cf. UK Department of Digital, Culture Media & Sport, 'Security of Network and Information Systems' Government Response to Public Consultation (January 2018); European Commission, 'Impact Assessment Report' SWD(2020) 345 final, Mark D. Cole and Sandra Schmitz, 'The Interplay between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape' [2019] University of Luxembourg Law Working Paper No. 2019-017). As regards cybersecurity incidents, these will in most scenarios require notification under the two regimes; hence, undertakings may face sanctions under different regimes in case of non-compliance. If, for example, a data controller fails to report a cyber incident to the national DPA and the competent NIS authority, the penalties relate to different aspects of the failure or different impacts (integrity of the service and protection of personal data). However, considering the potential quantum of fines with the highest fines introduced in the UK with an alignment to the GDPR penalty, undertakings, in theory, could face a maximum penalty of two times EUR 20,000,000.00 for one single incident. The UK legislator, which introduced the highest maximum fines when transposing the NIS Directive, thus, requires NIS enforcement authorities to consider whether the contravention is also liable to enforcement under another enactment (see section 23(e) of the UK Network and Information Systems Regulation 2018). However, not every national transposition addresses the risk of double jeopardy.

3. Processing of Personal Data in Accordance with the GDPR

The sharing of information on risks and incidents within the information sharing frameworks set up by the NIS Directive (e.g. within the CSIRTs network) may require the processing of personal data (see Recital 72). Recital 63 NIS Directive specifies that, in cases where personal data are compromised as a result of incidents, competent authorities under the NIS Directive and data protection authorities must cooperate and exchange all relevant information. Accordingly, Article 8(6) NIS Directive foresees that the competent NIS authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national DPAs. Article 15(4) NIS Directive further requires the competent NIS authorities to work in close cooperation with DPAs when addressing incidents resulting in personal data breaches. However, there is no statutory authorisation in neither the NIS Directive nor the GDPR nor the Law Enforcement Directive (Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89) to for instance process and transmit personal data within and between CSIRTs and business entities (see Kurt Einzinger and Florian Skopik, 'Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken' [2017] 41 Datenschutz und Datensicherheit 572, 573).

The GDPR addresses the processing of personal data 'for the purposes of ensuring network and information security' by public authorities, CERTs/CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, stating in Recital 49 that the processing of personal data to the extent necessary and proportionate for the purposes of ensuring network and information security by these actors constitutes a legitimate interest of the data controller concerned. While Recital 49 GDPR does not explicitly authorise processing of personal data by these actors, the reference to the 'legitimate interest' in the meaning of Article 6(1)(f) GDPR indicates that this data processing should be lawful. However, OESs and DSPs not necessarily fall within the categories of processors mentioned in Recital 49, for instance a private electricity undertaking, which carries out the function of energy supply, is neither a public authority, nor a CERT/CSIRT, nor a provider of electronic communications networks and services or a provider of security technologies and services. It has been argued that the processing of personal data by entities outside the scope Recital 49 in the form of transmitting personal data to CERTs/CSIRTs or national competent NIS authorities in the context of incident reporting must consequently either be regulated in national law, or based on consent of the data subject concerned (see Kurt Einzinger and Florian Skopik, 'Über die datenSchutzrechtliche Problematik in CERTs/CSIRTs- Netzwerken' [2017] 41 Datenschutz und Datensicherheit 572, 574 et seq.). It has also been argued that the transmission of data including personal data in the context of incident reporting constitutes a legitimate interest insofar as the transmission of that personal data

is necessary for the fulfilment of the incident reporting obligation (cf. ibid, 575). The reluctance to address the processing and transmission of personal data within and between reporting entities and CERTs/CSIRTs may be based on the assumption that the notification in cases of security incidents are of a mere technical natures, and may not necessarily contain personal data. In that line, the explanatory memorandum to the German BSIG (Act on the Federal Office for Information Security) states that notifications under § 8b BSIG will usually be of a mere technical nature and as a general rule are unlikely to relate to individuals. In general, the national implementations of the NIS Directive do not specifically address the transmission of personal data between OESs/DSPs and competent authorities. Moreover, they regular consider that the processing of personal data under the national NIS law shall be conducted in compliance with the GDPR and national data protection law.

Article 2(2) Processing of Personal Data in Accordance with the EU Institutions Data Protection Regulation

1. Introductory Remarks

The revision of the EU data protection framework also resulted in a new framework for the processing of personal data by EU institutions, bodies and agencies. 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 ([2001] OJ L008/1) as well as Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties ([2002] OJ L183/1) were repealed by the EU Institutions Data Protection Regulation (Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies and agencies and on the free movement of such data, [2018] OJ L295/39). Article 99 EU Institutions Data Protection Regulation provides that references to the repealed Regulation and Decision are to be construed as references to the EU Institutions Data Protection Regulation.

In the interest of a coherent approach of personal data protection throughout the EU, the EU Institutions Data Protection Regulation allows its application in parallel with the GDPR.

2. The Relationship between the NIS Directive and the EU Institutions Data Protection Regulation

The sharing of information on risks and incidents within the information sharing frameworks set up by the NIS Directive (e.g. within the CSIRTs network) may require the processing of personal data (see Recital 72). This processing should comply with the EU Institutions Data Protection Regulation. Similar to the processing of personal data in compliance with the GDPR, the NIS Directive does not further specify rules on data processing in accordance with the EU Institutions Data Protection Regulation.

III. Review of the NIS Directive

During the review process, also the interplay between the NIS Directive and the GDPR was addressed. In this regard, the focus was put on the fact that further clarifications are needed as regards the lawful data processing by the addressees of obligations under the NIS Directive. Further, the review process considered that most security incidents will involve some personal data, meaning that OESs and DSPS will have to report these incidents to both competent authorities in order to ensure compliance with both regulatory requirements (see European Commission, 'Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665' Final Study Report, pp. 103, 126).

IV. Outlook: The NIS 2 Directive

Besides general statements on cooperation and information exchange between DPAs and competent authorities under the NIS Directive (cf. Article 28(2) and Recital 108 NIS 2 Directive), the NIS 2 Directive addresses various forms of personal data processing in the recitals. First of all, Recital 43 NIS 2 Directive recognises that CSIRTs should be able to provide, in accordance with the GDPR, 'upon the request of an essential or important entity, a proactive scanning of the network and information systems used for the provision of the entity's services'. Pursuant to Article 11(3)(e) NIS 2 Directive, one of the tasks of CSIRTs will be said scanning of the network and information systems upon request of an essential or important entity. Member States have to ensure that this tasks can be conducted in line with the GDPR.

While Recital 26 of the Commission Proposal for a NIS 2 Directive only addressed the participation of CSIRTs in international cooperation networks in addition to the CSIRTs network established by the NIS Directive, the amendments following the trilogue negotiations that are now enshrined in Article 45 NIS 2 Directive, pay regard to the fact, that such participation may also include the exchange of personal data. Any information exchange of CSIRTs and competent authorities with CSIRTs of third countries or their authorities has to meet the conditions of transfer of personal data to third countries, for example those of Article 49 GDPR (see Recital 45 NIS 2 Directive).

Recital 121 NIS 2 Directive clarifies that the processing of personal data, 'to the extent necessary and proportionate for the purposes of ensuring security of network and information systems by essential and important entities, could be considered to be lawful on the basis that such processing complies with a legal obligation to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679'. In addition, said Recital notes that the processing of personal data 'could also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the

voluntary notification of relevant information in accordance with' the NIS 2 Directive. During the trilogue negotiations the list of examples for measures that could constitute a legal obligation or could be considered to be necessary for carrying out a task in the public interest, or in the exercise of official authority vested in the controller, or for pursuing a legitimate interest of the essential or important entities in the sense of Article 6(1) GDPR saw various amendments. The list encompassed in Recital 121 now enshrines a detailed non-exhaustive list of measures including 'measures related to the prevention, detection, identification, containment, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated vulnerability disclosure, the voluntary exchange of information about those incidents, and cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses and, where they reveal personal data, time stamps'. The legislator recognises that such measures may require the processing of IP addresses, uniform resources locators (URLs), domain names, and email addresses, which all constitute personal data. During the trilogue negotiations, it was agreed to amend Recital 69 of the Proposal (now: Recital 121) by also addressing that the 'processing of personal data by competent authorities, SPOCs and CSIRTs, could be considered necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller' pursuant to Article 6(1)(e) GDPR. The processing of personal data by said entities could further constitute a legal obligation pursuant to Article 6(1)(c) and Article 6(3) GDPR, or 'for pursuing a legitimate interest of the essential and important entities, as referred to in Article 6(1)(f)' GDPR. Furthermore, the legislator considers that Member States could 'lay down rules allowing the competent authorities, the single points of contact and the CSIRTs,…, to process special categories of personal data in accordance with Article 9 [GDPR], in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued'.

Recital 136 NIS 2 Directive addresses the aforementioned missing cooperation rules between the competent authorities and data protection authorities by clarifying that the NIS Directive should establish cooperation rules to deal with infringements related to personal data.

Article 35 NIS 2 Directive also introduces an obligation for NIS authorities to forward indication that an infringement of the reporting and security requirements imposed upon essential and important entities entails a personal data breach to the competent supervisory authorities under the GDPR.

Finally, the EU legislator also acknowledges that entities are often in a situation where a particular incident needs to be reported to various authorities as a result of notification obligations included in various legal instruments (see in that regard NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting' [2020] CG Publication 04/2020; as well as Sandra Schmitz-Berndt and Fabian Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context' [2021] (7)1 EDPL 101). Considering the additional administrative burden in filing multiple notifications, to which different formats and procedures may apply, Member States are encouraged in Recital 106 NIS 2 Directive to establish a single entry point for all notifications required under the NIS Directive and also under other Union law such as the GDPR and the E-Privacy Directive (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, OJ [2002] L201/37). In addition, ENISA, in cooperation with the NIS Cooperation Group, is called upon to develop common notification templates by means of guidelines to simplify and streamline the information to be reported under Union law.

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.

I. General Remarks

The legal basis for the NIS Directive is Article 114 TFEU (Treaty of the Functioning of the European Union, consolidated version, OJ [2012] C326/47) which provides a very versatile legislative basis for the issuance of legislation that serves the aim of smoothening the functioning of the internal market. According to Article 114 TFEU, the EU can adopt '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 original Commission Proposal for a NIS Directive (COM/2013/048 final) is based on the finding that NIS play an essential role in facilitating the cross-border movement of goods, services and people. In recognition of the intrinsic transnational dimension NIS, the Commission argued that the resilience and stability of NIS is essential to the smooth functioning of the internal market because a disruption in one Member State can also affect other Member States and the EU as a whole. With the Proposal for a NIS Directive, the European Commission also sought to eliminate the disparities resulting from uneven NIS national capabilities, policies and level of protection across Member States that led to barriers to the internal market and justifies EU action (see COM/2013/048 final). The legislator also concluded that a non-intervention at EU level 'would lead to a situation where each Member State would act alone, disregarding the interdependencies among EU network and information systems'. Accordingly, the NIS Directive seeks to ensure an appropriate degree of coordination among the Member States, address divergences in national NIS regulations that represent a barrier to trade, create a level playing field, and close legislative loopholes in NIS regulation (see COM/2013/048 final).

In accordance with the principle of proportionality, the explanatory memorandum of the Proposal for a NIS Directive stresses that the proposed Directive does not go beyond what is necessary in order to achieve those objectives. For the EU's limited mandate to regulate cybersecurity, see Mark D. Cole and Sandra Schmitz-Berndt, 'Towards an efficient and coherent regulatory framework on cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act' [2022] ACIG 1, DOI 10.5604/01.3001.0016.1323.

The choice of the instrument of a directive enables Member States to take account of national specificities – as long as it does not follow a maximum harmonisation approach.

The harmonisation of national rules by way of an EU directive issued on the basis of Article 114 TFEU may basically take two forms: minimum harmonisation or maximum harmonisation. Both approaches can contain options, alternatives or only partially cover a certain field of law. While the Commission Proposal for a NIS Directive proposed a full minimum harmonisation approach, the NIS Directive as adopted in 2016 employs a minimum harmonisation approach but exempts from this minimum harmonisation the security or notification requirements on DSPs. The latter pays regard to the fact that DSPs have per se a cross-border nature and thus require a more harmonised approach (see Recital 49). However, taking into consideration that the legislative proposal was based on the finding that there is an 'intrinsic transnational dimension of network and information systems', the choice for differentiation between minimum and maximum harmonisation seeks to balance the regulatory interests of the EU with the interests of Member States where the protection of essential, and thus critical, infrastructures also touch upon national security.

II. In Detail

1. Minimum Harmonisation Approach towards OESs

As regards the harmonisation to be achieved, a directive may set minimum standards (minimum harmonisation approach). Minimum harmonisation instruments do not set a mandatory rule as both floor and ceiling, but rather only a floor that allows Member States to maintain or introduce stricter rules, up to the ceiling set by EU primary law (cf. Stephen Weatherill, 'The Fundamental Question of Minimum or Maximum Harmonisation' in: Sacha Garben and Inge Govaere (eds), *The Internal Market 2.0* (Hart Publishing 2020) 261). Pursuant to this principle, Member States may adopt or maintain a provision with a view to achieving a higher level of NIS security that goes beyond the standard set by the NIS Directive. Accordingly, Member States may for example include more sectors and services than those covered in Annex II and III of the Directive or even expand the security and notification obligations under Article 14 of the Directive.

By employing the minimum harmonisation approach towards OESs, the Directive recognises the fact that the legal systems in some EU Member States already may entail higher standards, or may aim for higher standards than those foreseen under the Directive.

In fact, various Member States have decided to include additional sectors (e.g. public administrations, postal sector, food sector, chemical and nuclear industry) and expand the obligations for the sectors covered. This may then also be reflected in the respective national cybersecurity strategy (see European Commission, 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). The minimum harmonisation approach also meant that Member States were given leeway in determining which entities meet the criteria of the definition of OESs, i.e. inter alia

which services are considered as essential for the maintenance of critical societal and economic activities (see Article 5(2) NIS Directive). Furthermore, the means to assess compliance and ensure enforcement of reporting and security requirements vary across Member States.

2. Maximum Harmonisation Approach towards DSPs

In the case of maximum harmonisation, EU Member States may not introduce rules that are stricter than those set in the respective directive; maximum harmonisation can thus be compared to mandatory rules which must be followed without deviations. Accordingly, norms of national law implementing the NIS Directive must be identical as to their scope and effect.

With Article 16(10) setting forth that 'Member States shall not impose any further security or notification requirements on digital service providers', the maximum harmonisation approach towards DSPs is limited to exactly these requirements.

III. Review of the NIS Directive

The NIS Directive left some freedom to the Member States as far as the implementation and achievement of the Directive's objectives are concerned.

The Final Study Report to support the review of the NIS Directive (European Commission et al., Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665, p. 12) concluded that the minimum harmonisation approach regarding OESs combined with the diverse cyber maturity levels of Member States and the lack of clarity concerning the definition of OESs, resulted in a lack of harmonisation in the OESs identification process across the EU. In fact, the identification process of OESs turned out to be inconsistent (ibid, p. 24). The Study also identified great variation as regards the thresholds for incident reporting, supervision and the type and level of penalties (ibid, pp. 15 et seq.). In particular the lack of harmonisation in OESs identification led to 'distorted competition, as companies of the same nature might be imposed different requirements depending on the Member State where they operate' (ibid, p. 46). Distorted competition however does not align with the rationale of the single market.

In recognition that asymmetries in relation to OESs provisions create a risk of fragmentation in the internal market, the Study addressed the need for more harmonisation regarding the identification process of OESs and incident reporting thresholds.

IV. Outlook: NIS 2 Directive

The NIS 2 Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ [2022] L333/80) strives for a higher level of harmonisation. While the general

approach of minimum harmonisation is maintained in Article 5 NIS 2 Directive, the Directive provides for targeted improved harmonisation by establishing generally applicable rules on the scope of application of the NIS Directive, harmonising the rules applicable in the area of cybersecurity risk management and incident reporting. In that regard, it must be noted that the NIS 2 Directive abandons the distinction made between OES and DSPs and, in turn, introduces a differentiation between 'essential' and 'important' entities that takes into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services (Article 3). By applying the same cybersecurity risk management requirements (see Article 21 NIS 2 Directive) and reporting obligations (see Article 23 NIS 2 Directive), there is also no longer a different level of harmonisation applying to different types of service providers.

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.

I. General Remarks

The NIS Directive does not define explicitly which particular entities will be considered as OESs under its scope. Instead the NIS Directive provides in its Annex II a list of seven sectors and their respective sub-sectors including types of entities which are relevant for the identification process of OESs. Member States must assess for each sector and subsector referred to in Annex II, which services are considered as essential for the maintenance of critical societal and economic activities. In that regard each Member State must assess whether the operators of services listed in the Annex meet the criteria for the identification of OESs enshrined in Article 5(2). The fact that an operator provides a service listed in Annex II does not imply that this operator is an OES. The identification of OESs is a national issue, i.e. Member States have to identify the operators with an establishment on their territory and establish a list of the services identified. Since Article 5(2) only sets forth the criteria for the identification, but does not set thresholds, Member States are given large discretion as to how they apply the criteria and identify OESs. In recognition that in the internal market many OES operate in more than one Member State, Article 5(4) foresees a consultation procedure before a decision on identification is taken. Member States are required to update the lists of identified OESs on a regular basis (Article 5(5)). In order to ensure a consistent approach in the identification of OESs across the Union, the Member States are supported by the Cooperation Group (Article 5(6)). When assessing the implementation of the Directive, the European Commission also assesses said consistency. For this process, Member States must provide the Commission with the necessary information (Article 5(7)).

II. In Detail

Article 5(1) Identification of OES with an Establishment on a Member State's Territory

Article 5(1) NIS Directive stipulates that by 9 November 2018, Member States shall have completed their identification process of OESs.

In the process of identification of OESs, Member States should assess, at least for each subsector referred to in the Directive, which services must 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 the Directive and providing those services meet the

criteria for the identification of operators (Recital 20). The minimum harmonisation approach of the NIS Directive allows Member States to carry out identification in sectors and subsectors additional to those listed in Annex II. Some Member States have extended the scope of their NIS law to cover additional sectors and subsectors: the sectors include inter alia business services for government bodies (Croatia), chemical industry (Czechia), public broadcasting (Estonia), logistics (France), social security (France), waste water (France), education (France), food (France, Germany, Slovenia) and environmental protection (Slovenia).

When Article 5(1) NIS Directive requires Member States to identify OES with an establishment in their territory, this does not mean that the competent authorities (Member States may have more than one competent authority, see commentary to Article 8 NIS Directive) have to identify the operators themselves. In fact, two different approaches are employed across Member States: top-down (also referred to as state-driven) or bottom-up (also referred to as operator-driven). In the top-down approach the leading role is in most cases assumed by one or more governmental agencies/ministries that are mandated to identify the essential services and OES. In the bottom-up approach, OES have to self-identify meaning that they have to self-assess if specific criteria are met and then register to the list of OES. France, for instance, employs a top-down approach: in the designation process, as a first step, the French national NIS authority ANSSI issues a letter of intention to each potential OES indicating that the operator is proposed to be designated as OES and requesting information whether service is provided in any other Member State (Article 3 Décret no 2018-384 du 23 mai 2018 relatif à la sécurité des reseaux et systems d'information des opérateurs de services essentiels et des fournisseurs de service numérique). The operator concerned is granted a period of one month to respond to the letter of intention. OES are designated by order of the Prime Minister. A similar approach is employed in Ireland: the competent authority informs an operator of a potential essential services about the intention to designate the operator as OES. The letter of intention includes the reasons why the operator is proposed to be designated and the respective (sub-)sector as well as granting the right to make representations in respect of the proposed designation (Article 13(2) European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018) Any representations made will be considered when deciding upon the designation (ibid, Article 13(3)). In contrast to France and Ireland, Germany operates a bottom-up approach where categories of facilities and industry-specific threshold values for each sector and sub-sector are set forth in a regulation (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz).

For the purposes of OES identification, an establishment in a Member States implies the effective and real exercise of activity through stable arrangements, irrespective of the legal form of such arrangements (Recital 21 NIS Directive). This connecting factor has been interpreted by Member States in different ways. For instance, German law does not replicate the notion of 'establishment' but introduces the notion of 'facility'. A 'facility' is defined as a 'permanent establishment and other fixed equipment required for the provision of an essential service' and 'machinery, devices, and other fixed equipment required for the

provision an essential service' (§ 2 X BSIG and § 1 I no. 1 BSI-KritisV; see also Dennis-Kenji Kipker, *Cybersecurity* (1st edn, Beck 2020), p. 370). Accordingly, it is sufficient that infrastructure of the operator is located within the territory of a Member State. Instead of the mere location of fixed equipment, in Poland, Article 5.1 USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa requires that the entity has an 'organisational unit' in Poland. A stricter approach to 'establishment' is taken in Spain, when it is required that the company has its residence or its registered office within Spanish territory provided that this coincides with the place where the administrative management and the management of its businesses or activities are effectively centralised (Article 2(2)(a) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información). The Italian transposition of the NIS Directive requires that the company is domiciled in Italy (Article 4(1) Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione). These divergent interpretations of 'establishment' can result in some entities being identified as OESs in some Member States but not in others.

In view of the foregoing, it follows that companies identified as OESs will be subject to the jurisdiction of the Member State where they provide essential services. Additionally, if those companies provide essential services in more than one Member State, they will be subject to the jurisdiction of each of those Member States in parallel. Thus, several Member States can concurrently have jurisdiction over the same OES if, for example, the operator has branch offices — or anything that amounts to an establishment under domestic law (see above) — in different Member States (European Commission, 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, Annex 1, sec. 4.1.4). Moreover, as the NIS Directive follows a minimum harmonisation approach regarding OESs, Member States are free to impose requirements on OESs that are higher than those provided for in the Directive (European Commission, 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). Consequently, companies identified as OES in more than one Member State will need to comply with security and reporting requirements that may vary greatly across countries (cf. commentary to Articles 14 and 16). By way of illustration, Ryanair is headquartered in Ireland and is reportedly the biggest airline in seven EU countries (Ireland, Spain, Italy, Poland, Lithuania, Slovakia, and Bulgaria), the second biggest in five more (Portugal, Belgium, Hungary, Czech Republic, and Latvia), and the third biggest in the UK (see Johan David Michels and Ian Walden, 'How safe is safe enough? Improving cybersecurity in Europe's critical infrastructure under the NIS Directive' [2018] Queen Mary School of Law Legal Studies Research Paper No. 291/2018, p. 10. This means that Ryanair could potentially be identified as an OES in 13 different countries, and consequently it would have to interact with the NIS

national competent authorities (NCAs, SPOCs, CSIRTs and sector-specific authorities) of each of those jurisdictions. In addition, Ryanair would have to implement the security measures and comply with the reporting obligations specified in the national transposition measures of each of the countries where it provides its services, which may vary in terms of reporting thresholds, timeframes, content, and formal requirements, and may even present consistency problems (ibid).

Article 5(2) Criteria for the Identification of OESs

The NIS Directive does not define explicitly which entities will be considered as OESs. Instead, Member States have to implement an identification process. Article 5(2) NIS Directive sets forth three criteria to be applied by Member States in this process, namely, that (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.

Responsibility in determining which entities meet the criteria listed in Article 5(2) NIS Directive rests with the Member States. The rather general criteria reflect the minimum harmonisation approach taken towards OESs. Member States are given room for manoeuvre in selecting entities to account for national specificities (European Commission, 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, sec. 1.1.3).

Recital 20 specifies that 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. As regards the requirement of dependence on NIS, it should be demonstrated that provision of the essential service is dependent on NIS. The notion of NIS is defined in Article 4(1) NIS Directive. Further, when assessing whether an incident would have a significant disruptive effect on the provision of the service, Recital 20 requires Member States to take into account a number of cross-sectoral factors, as well as, where appropriate, sector-specific factors. As regards for example such sector-specific factors in the water transport sector, Recital 11 specifies that 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.

In relation to the identification process, the European Commission provides some general guidance in a Communication (European Commission, COM(2017) 476 final, Annex I, sec. 4.1.6). The Communication lists six key questions that a national authority should examine step-by-

step when carrying out the identification process concerning a particular entity. These questions are:

(1) Does the entity belong to a sector/subsector & correspond to the type covered by Annex II of the Directive?; (2) Is a lex specialis applicable?; (3) Is the operator providing an essential service within the meaning of the Directive?; (4) Does the service depend on a network and information system?; (5) Would a security incident have a significant disruptive effect?; and (6) Is the operator concerned providing essential services in other Member States?.

Basically, these questions repeat the requirements set forth in the Directive and places them into a logical order. The step-by-step approach also reminds national NIS authorities to assess whether the provision of lex specialis enshrined in Article 1(7) NIS Directive applies.

While the assessment of Article 5(2)(a) and (b) NIS Directive and questions (1) to (4) seem rather straightforward, the practice in Member States shows that divergences prevail. These divergences are the result of differences in national methodologies to identify operators. Some Member States already had methodologies in place prior to the NIS Directive (e.g. Germany with the Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) which they then adapted to the specificities of the NIS Directive (see European Commission, 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). The European Commission Report on the consistency of the OES identification approaches identifies the degree of centralisation as one reason for diverging approaches. Degree of centralisation refers to the designation of who renders decisions as regards various elements of the identification process. Some Member States have delegated elements of the identification process to sectoral authorities (ministries, agencies etc.), while other Member States have tasked one single authority with the identification process. Where sectoral authorities are in charge, most Member States have tasked one authority with providing guidance to the sectoral authorities (see ibid, sec. 2.1). However, there are also Member States with a high degree of decentralisation where the sectoral authorities are responsible for developing their own methodologies. With many different actors defining national (sectoral) methodologies, divergences are immanent.

Member States are also employing different approaches when it comes to who determines whether the criteria of Article 5(2) under the national identification methodology are fulfilled. In some Member States, national competent authorities carry out the identification process (top-down identification), whereas in other Member States the entities have to self-identify (bottom-up identification) whether they are to be considered an OES (see ibid, sec. 2.1).

As regards the first step of the identification process, namely, whether an operator belongs to a sector/subsector and corresponds to the type covered by Annex II NIS Directive, the

assessment depends to a large extent on the level of granularity in service identification. Member States apply different levels of granularity, meaning that some provide a list of detailed services they consider as essential whereas other Member States operate with more general headings leaving room for interpretation. Taking the example of the energy sector, Estonia, for instance, employs a very general approach whereby in the energy sector any entity that supplies electricity is considered an entity of a type referred to in Annex II NIS Directive (see ibid, sec. 2.2, table 2). In contrast, Bulgaria, which employs the most granular approach, differentiates between different actors in the electricity sector and provides a detailed list of services. Member States with a less granular approach may haven chosen to include services that other Member States have not included (see ibid, sec. 2.2, table 2). While some Member States may only define the sector (least granular approach), there are also Member States that have left out a particular sector from their list of essential services or have not identified entities in a particular sector. Exemplary for this is the health sector: the Netherlands did not identify the healthcare sector as OESs at all (see Besluit beveiliging network- en informatiesystemen); a reason for this may be the highly decentralised nature of the healthcare system with many small operators, which provide an essential service to a relatively low number of users. However, the health sector is not limited to the treatment of patients; Member States have identified a large variety of services as essential including the supply of pharmaceutics, blood and plasma concentrates and laboratory diagnostics (e.g. Germany, Luxembourg). Due to the different levels of granularity, the lists of essential services are difficult to compare and result in fragmentation, when for instance all hospitals in one Member State (e.g. Luxembourg) are covered by the NIS law, while in a neighbouring Member State (the Netherlands) no hospitals at all fall under the scope of the Directive. Similarly in the banking and financial sector, a few Member States refrained from identifying OES based on the presumption that operators are providing services covered by lex specialis (European Commission, 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, sec. 2.7).

The different levels of detail in the description of services may lead to consistency gaps. This is also the case, where Member States list categories where it is not sufficiently clear, which services fall under a category (see ibid, sec. 2.2 with reference to the Polish list of categories in the railway sector).

As regards the assessment of an operator's dependence on NIS (Article 5(2)(b) NIS Directive), many Member States consider dependence on NIS to be inherent in the digital economy. However, the Commission Report on the consistency of approaches taken identifies more elaborate practices employed by some authorities; for example some authorities conduct detailed assessments or require operators to self-evaluate the degree of their dependence (see ibid, sec. 2.1).

In contrast to questions (1) to (4), question (5) on the significant disruptive effects of a security incident is rather challenging. As regards the hypothetical question whether an incident would have a significant disruptive effect on the provision of the service, Article 6(1) NIS Directive lays down several cross-sectorial factors that need to be taken into account in the assessment. In addition, Article 6(2) NIS Directive requires the consideration of sector-specific factors if appropriate (see Article 6 NIS Directive). In order to facilitate identification of services where an incident would have significant disruptive effect, Member States have introduced national thresholds (see also commentary to Article 6 NIS Directive). These different thresholds again contribute to fragmentation across the EU with operators in one Member State potentially being exposed to additional regulation, while others providing identical or at least similar services in other Member States are excluded. The thresholds applied by Member States to identify OESs vary between Member States and can be cross-sectoral or sector-specific. Since the thresholds depend on the factors that Member States take into consideration to identify OESs, the different approaches are outlined in the commentary to Article 6 NIS Directive. At this point, it shall be noted that where cross-sectoral thresholds are set up, these can be distinguished as follows: thresholds relying on (1) a single quantitative factor (e.g. number of users relying on the service); (2) a larger set of quantitative factors (e.g. number of users relying on a service + market share); (3) a combination of quantitative and qualitative factors (see ibid, sec. 2.3).

For the assessment of service provision in other Member States see below the comment on Article 5(4) NIS Directive.

Article 5(3) List of Services

Article 5(3) requires each Member State to establish a list of essential services based on the sector, subsectors and types of entities listed in Annex II. There is great variation in the numbers of services identified by Member States and have been reported to the Commission by November 2018: the number of identified services in 2019 ranged from 12 to 87 (European Commission, 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, sec. 4.2). According to the data collected by the European Commission (ibid), the number of identified services is as follows: 87 (Poland), Romania (77), France (70), Spain (55), Croatia (49), Austria (46), Denmark (39), Italy (37), Lithuania (37), Slovenia (34), Belgium (31), Czech Republic (31), Bulgaria (30), Greece (30), Cyprus (29), Malta (29), Slovakia (28), Sweden (27), Ireland (26), Portugal (26), Luxemburg (21), Finland (20), Estonia (18), Latvia (18), Germany (15), Hungary (12), the Netherlands (12). In general, the number of identified services per Member States varies significantly. For instance, in the banking sector, the number of identified services range from 1 to 21 (see ibid, sec. 2.2).

The discrepancy in numbers is a direct result of the different approaches to identification of services. Generic approaches resulted in less essential services identified than in Member States that have chosen a granular method.

As of November 2018, eleven Member States identified further essential services in addition to those foreseen under the NIS Directive: France (20 additional services), Spain (18), Cyprus (17), Czech Republic (12), Germany (12), Slovakia (7), Estonia (6), Bulgaria (3), Croatia (2), Malta (2), Slovenia (2) (ibid).

Article 5(4) Cross-Border Consultation Procedure

The Commission advises the Member States to already consider in the identification process whether an operator identified as OES provides essential services in more than one Member State (European Commission, COM(2017) 476 final, Annex I, sec. 4.1.6). This step pays regard to Article 5(4) NIS Directive which requires the concerned Member States to engage in a consultation process.

If an entity provides an essential service in more than one Member States, before the decision on the identification is taken, the Member States concerned must engage in consultation with each other. Recital 24 clarifies that the purpose of the consultation process is to help them to assess the critical nature of the operator in terms of cross-border impact, allowing each Member State involved to present its views regarding the risks associated with the services provided.

The background is that cross-border OESs must deal concurrently with a multiplicity of national competent authorities in each of the different countries where they provide services that are considered essential. They may need to sort out an uneven landscape regarding applicable security and reporting obligations if they are identified as an OES in more than one Member State.

The purpose of the consultation procedure is to avoid unnecessary divergence or inconsistencies in the application of the NIS Directive, but also to help Member States to assess the potential impact of a cyber-incident affecting entities operating across borders as well as acting as safeguard for the companies affected by the procedure in different Member States (see European Commission, COM/2019/546 final).

To date, there is no established process to facilitate the consultation process (see also NIS Cooperation Group, Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact, CG Publication 07/2018, 9). The NIS Cooperation Group published the aforementioned non-binding reference document that seeks to establish the modalities for a consultation process. The NIS Cooperation Group considers the SPOC as the key national entity to undertake the consultation on behalf of each Member State involved since SPOCs shall exercise a liaison function in cross-border cooperation under Article 8(4). The reference documents sets out a

five step procedure for the consultation. Once the originating Member State (i.e. a Member State on whose territory the OES in question is located) or the affected Member State (i.e. a Member State which is potentially affected by the loss of an essential service originating from an operator located in another Member State) has identified that an OES provides service in both or more Member States, the originating and the affected Member State have the same right to the consultation. The Cooperation Group suggests that the originating state initiates the consultation process (ibid). As a second step, the OES shall submit to the originating Member State's SPOC a list of information (for the content required see ibid, 12). As a third step, based on the information received, the originating Member State's SPOC sends appropriate information (cf. ibid, 13) to each Member State engaged in the cross-border service provision (ibid, 12). Affected Member States are free to request more information or request for an individual consultation with the originating Member State's SPOC (ibid). If the involved SPOC consider that the information provided is sufficient, each SPOC may forward the final set of information to the national competent authority, which draws up the list of OES (ibid). In a fifth and final step, the national competent authority assess the information and decides whether to update the national list of OESs (ibid). Where the OES is considered to have an establishment in the territory of the affected Member State, the national competent authority may inform the OES about the result of the consultation process (ibid). Where the OES concerned is also an operator of an European critical infrastructure, the already existing procedures including those mentioned in Article 4 ECI Directive must also be taken into account (ibid).

In practice, some Member States have been using this consultation process simply as a notification exercise, while other considered the procedure as a means to align regulatory requirements (European Commission, COM/2019/546 final). It turned out that often Member States were not able to coordinate the consultation process with two Member States at the same time (ibid).

Article 5(5) Review of the List of OESs

Article 5(5) NIS Directive requires Member States to ensure that the list of identified OESs is kept up to date. Accordingly, Member States have to review and, where appropriate, update the list, at least every two years after 9 May 2018.

Article 5(6) Role of the NIS Cooperation Group

In order to support the Member States in the identification process, the NIS Cooperation Group (NIS CG) published a reference document on the modalities of the consultation process in cases with cross-border impact (NIS Cooperation Group, Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact, CG Publication 07/2018). Furthermore, in accordance with Article 24(2), the NIS CG is to discuss the process, substance and type of national measures allowing for the OES identification in specific sectors.

Prior to the completion of the identification process, Member States may also consult the NIS CG to discuss its draft national identification measures (see ibid).

Article 5(7) Assessment of the Implementation of the Directive – Consistency of Member States' Approaches

Article 5(7) NIS Directive requires Member States to provide to the European Commission information on (a) national measures allowing for the identification of OES; (b) the list of essential services; (c) the number of identified OES for each sector and the relevance of those operators for the sector; (d) 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. This information is not publicly available.

Article 5(7) prescribes that all Member States provide this information for the purpose of the review referred to in Article 23 (European Commission, COM/2019/546 final) no later than 9 November 2018. As regards this first report, there was a significant reluctancy on behalf of some Member States to provide the requested data. Only 15 Member States complied with this obligation by submitting substantial data to the Commission by November 2018. Following repeated reminders, the Commission sent out letters of formal notice in July 2019 to six Member States (Austria, Belgium, Greece, Hungary, Romania and Slovenia) of which data was missing (see ibid).

The data provided by Member States turned out to be difficult to compare due to the different methodological approaches in the identification of services and OES. Diverging interpretation by Member States as to what constitutes an essential service under the NIS Directive and the different levels of granularity applied resulted in a such a level of diversity that the potential negative impact on achieving the Directive's goals could be identified in the first Commission Report on the consistency of approaches.

III. Review of the NIS Directive

Already during the transposition period of the NIS Directive, the European Commission stressed the importance of a maximum alignment of national identification procedures in order to achieve a harmonised application of the Directive's provisions and to reduce the risk of market fragmentation (European Commission, COM(2017) 476 final). However, a subsequent assessment of the consistency of approaches revealed significant fragmentation (see European Commission, COM/2019/546 final). This fragmentation resulted from the different variety of methodologies for OES identification outlined above including determination by national competent authorities and self-identification by the operators themselves, which in turn is a result of the minimum harmonisation approach (European Commission et al., Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 020-665, p. 12). The divergent identification procedures can result in some entities being identified as OESs in some Member States but not in others which, in turn, may result

in an uneven level of cyber-resilience between different Member States and lead to distorted competition, as companies of the same nature might be imposed different requirements depending on the Member State where they operate (ibid, p. 46). As regards entities that operate cross-border in more than one EU Member State, only few Member States have engaged in cross-border consultation before defining the criteria for the identification of OESs for the entities concerned (ibid, p. 14). By 2018, only two Member States had comprehensively contacted other Member States, some other Member States contacted other Member States in an unstructured manner (ibid, p. 14). Some Member States have been using the consultation process as a mere notification exercise, while others took the chance to align regulatory requirements (ibid). Difficulties in terms of coordination arose where the entity concerned operated in more than two Member States (ibid).

Where an operator that is established in more than one Member State, that operator may be faced with different procedures for OES identification with potentially different criteria/thresholds being applied to identify the establishment as OES that cause conflicts in terms of supervision.

IV. Outlook: The NIS 2 Directive

The NIS 2 Directive abandons the distinction made between OES and DSPs and, in turn, introduces a differentiation between 'essential' and 'important' entities that takes into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services (Article 3 NIS 2 Directive). Both categories are subject to the same risk management requirements and reporting obligations (Articles 21 and 23 NIS 2 Directive). However, they have different supervisory and penalties regimes (Articles 31 to 36 NIS 2 Directive).

In order to eliminate the wide divergences among Member States in OES identification and ensure legal certainty, the NIS 2 Directive introduces a uniform criterion that determines the entities falling within the scope of the Directive (see Recital 7 NIS 2 Directive). Accordingly, the identification process for essential and important entities is abolished and a general size-cap rule is introduced: entities of a type referred to in Annex I or II of the NIS 2 Directive which exceed the ceiling for medium-sized enterprises provided for in Article 2(1) of the Annex to Commission Recommendation of 6 May 2003 concerning the definition of micro, small, and medium-sized enterprises ([2003] OJ L124/36). This means that all entities of the types referred to in Annex I or II of the NIS 2 Directive that employ at least 50 persons and have an annual turnover and/or annual balance sheet total of at least EUR 10 million will be encompassed. In addition, Member States should also provide for certain small enterprises and microenterprises, as defined in Article 2(2) and (3) of that Annex, which fulfil specific criteria that indicate a key role for society, the economy or for particular sectors or types of service to fall within the scope of the NIS 2 Directive.

Regardless of their size, the NIS 2 Directive applies to entities of a type referred to in Annex I or II, where the services are provided by providers of public electronic communications networks or of publicly available electronic communications services (Article 2(2)(a)(i)) NIS 2 Directive, trust service providers (Article 2(2)(a)(ii)) NIS 2 Directive, top-level domain name registries and domain name system service providers (Article 2(2)(a)(iii) NIS 2 Directive); where the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities (Article 2(2)(b) NIS 2 Directive); where a disruption of the service provided by the entity could have a significant impact on public safety, public security or public health (Article 2(2)(c) NIS 2 Directive); where the disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact (Article 2(2)(d) NIS 2 Directive); where the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State (Article 2(2)(e) NIS 2 Directive); where the entity is a public administration entity of central government as defined by a Member State in accordance with national law (Article 2(2)(f)(i) NIS 2 Directive), or at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities (Article 2(2)(f)(ii) NIS 2 Directive).

Also regardless of their size, the NIS 2 Directive applies to entities that are identified as critical entities under Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive) ([2022] OJ L333/164) (Article 2(3) NIS 2 Directive), and entities providing domain name registration services (Article 2(4) NIS 2 Directive).

As an option, Member States may provide for the NIS 2 Directive to apply to public administration entities at local level (Article 2(5)(a) NIS 2 Directive), and education institutions, in particular where they carry out critical research activities (Article 2(5)(b) NIS 2 Directive).

In light of this enlarged scope of application the NIS 2 Directive provides for a number of exceptions. Accordingly, the NIS 2 Directive provides for the possibility to exempt public administration entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement (Article 2(7) NIS 2 Directive). Recital 8 NIS 2 Directive clarifies that public administration entities whose activities are only marginally related to those areas should not be excluded from the scope of the Directive. To ensure the protection of the essential interests of national security, to safeguard public policy and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences, Member States are able to exempt further specific entities which carry out activities in the aforementioned areas (Article 2(8) NIS 2 Directive).

The NIS 2 Directive distinguishes between essential and important entities. Essential entities (EEs) are those of a type referred to in Annex I which exceed the ceilings for medium-sized

enterprises provided for in Article 2(1) of the Annex to Commission Recommendation 2003/361/EC (Article 3(1)(a) NIS 2 Directive); qualified trust service providers and top-level domain name registries as well as DNS service providers (Article 3(1)(b) NIS 2 Directive); providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises (Article 3(1)(c) NIS 2 Directive); public administration entities of central government (Article 3(1)(d) NIS 2 Directive; any other entities of a type referred to in Annex I or II that are identified by a Member States as essential entities pursuant to Article 2(2)(b)-(e) of the Directive (Article 3(e) NIS 2 Directive); entities identified as critical entities under the CER Directive (Article 3(f) NIS 2 Directive); and if the Member State so provides, entities which that Member State identified before 16 January 2023 as OES in accordance with the NIS Directive or national law (Article 3(g) NIS 2 Directive). Those entities of a type referred to in Annex I and II to the NIS 2 Directive which do not qualify as essential entities shall be considered important entities (IEs); this includes entities identified by Member States as important entities pursuant to Article 2(2)(b) to (e) of the Directive (Article 3(2) NIS 2 Directive).

In order to ensure a clear overview of the entities falling within the scope of the NIS 2 Directive, Member States should establish a list of essential and important entities as well as entities providing domain name registration services by 17 April 2025 (Article 3(3) NIS 2 Directive). For that purpose, Member States should require entities to submit contact details to the competent authorities and, where applicable, the relevant sector and subsector referred to in the annexes, as well as, where applicable a list of the Member States where they provide services falling within the scope of the NIS 2 Directive (Article 3(4) NIS 2 Directive). As regards these obligations, the Commission with the assistance of ENISA are tasked to provide guidelines and templates (ibid). Member States are encouraged to establish national mechanisms for entities to register themselves (ibid).

The Member States are responsible for submitting to the Commission at least the number of essential and important entities for each sector and subsector referred to in the annexes, as well as relevant information about the number of identified entities and the provision on the basis of which they were identified, as well as the type of service that they provide by 17 April 2025 (Article 3(5) NIS 2 Directive).

When it comes to the jurisdictional rules, which are a prerequisite for identification of essential and important entities, the NIS 2 Directive provides that, as a rule, all essential and important entities will fall under the jurisdiction of the Member State where they provide their services (Article 26(1) and Recital 113 NIS 2 Directive). However, providers of public electronic communications networks or providers of publicly available electronic communications services should be considered to fall under the jurisdiction of the Member State in which they provide their services (Article 26(1)(a) NIS 2 Directive). DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network

providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms should be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union (Article 26(1)(b) NIS 2 Directive). Public administration entities should fall under the jurisdiction of the Member State which established them (Article 26(1)(c) NIS 2 Directive).

If the entity provides services in more than one Member State or is established in more than one Member State, it will fall under the separate and concurrent jurisdiction of each of these Member States. In this last case, the competent authorities of the different Member States should cooperate with each other and where appropriate, carry out joint supervisory actions.

In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, only one Member State should have jurisdiction over those entities. Jurisdiction should be attributed to the Member State in which the entity concerned has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective 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 that respect. Whether that criterion is fulfilled 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 decisive criteria for determining the main establishment. The main establishment should be considered to be in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken in the Union. This will typically correspond to the place of the entities' central administration in the Union. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment should be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment should be considered to be in the Member State where the entity has the establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings (Recital 114 NIS 2 Directive).

The general jurisdictional regime applicable to essential and important entities under the NIS 2 Directive is comparable to the one applicable to OES under the NIS Directive with the

advantage that it does not rely on the concept of establishment that, as it was mentioned above, can be and has been interpreted in different ways by Member States.

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.

I. General Remarks

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 (Recital 27 NIS Directive).

Article 6 lays down several cross-sectoral factors that have to be taken into account in the assessment of the significance of a disruptive effect in the meaning of Article 5(2)(c) NIS Directive. Further, Article 6(2) NIS Directive, requires, if appropriate, to take into account sector-specific factors.

Taking into account the factors to be considered, most Member States have set up thresholds to identify OESs. Where cross-sectoral thresholds are set up, these can be distinguished as follows: thresholds relying on (1) a single quantitative factor (e.g. number of users relying on the service); (2) a larger set of quantitative factors (e.g. number of users relying on a service + market share); (3) a combination of quantitative and qualitative factors (see European Commission, 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), sec. 2.3).

II. In Detail

1. Cross-Sectoral Factors

The cross-sectoral factors listed in Article 6(1) are the following:

(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.

As regards the number of users relying on the service, Recital 27 NIS Directive clarifies that the use of the service can be direct, indirect or by intermediation. Accordingly, the number of users to take into account is not necessarily restricted to, for instance, subscribers of a specific services, or customers of a specific provider. In addition, Recital 27 NIS Directive specifies that '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.

The cross-sectoral factors of Article 6(1) NIS Directive are replicated in many national transpositions without further amendments (e.g. § 16 NISG [Austria]; Article 13 § 2 Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique [Belgium]; Article 7 (2) Zakon o informacijski varnosi [Slovenia]). Some Member States refrained from listing the factors explicitly in the national implementation; instead, these Member States have set up individual thresholds for every service that takes into consideration the factors listed (see for instance BSI-KritisVO [Germany] and § 3 Küberturvalisuse Seadus [Estonia]).

The NIS Cooperation Group's Report on the sectorial implementation of the NIS Directive in the Energy Sector (CG Publication 03/2019) enlists some of the methods used to identify thresholds in the energy sector. The methods include inter alia national risk assessments and national exercises, as well as the identification procedure foreseen for critical infrastructures under the ECI Directive. Since the latter only applies to the energy and transport sector, the identification procedure is limited to these sectors. The Cooperation Group's Report also identifies some of the sources that Member States consulted in order to define which criteria to use for their OES identification approach; these sources include national statistics, expert

discussions, data from each sector via public-private partnerships and public data from a sector.

The Commission identified the diversity of approaches taken in its Report on the consistency of approaches taken (European Commission, 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) and concluded that the margin to manoeuvre in the identification process resulted in 'very complex mix of thresholds' that is likely to have a negative impact on overall OES identification consistency.

2. Sector-Specific Factors

Sector-specific factor allow national authorities to take account of national and sectoral specificities (see ibid, sec. 2.3).

As regards the sector-specific factors, recital 28 provides some guidance by outlining examples. Accordingly, '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'.

A comparison conducted by the European Commission in the digital infrastructures sector sheds light on the diversity of sector-specific approaches: while some Member States employ a quantitative approach with set thresholds for certain services (e.g. Germany, which requires that an Internet Exchange Points (IXP) provider manages more than 300 connected autonomous systems in order to be identified as OES; or Denmark, which requires an average daily data volume of more than 200 gbit/s), other Member States may require a certain market share (e.g. Malta 25 % market share; see ibid, sec. 2.3). Where the Member State employs a quantitative threshold, the reference point may also vary as can be seen for the provision of Top-Level-Domain registries: while some Member States set the threshold on domains registered (e.g. Austria, Denmark, Sweden), other Member States set the threshold on requests per day (e.g. Malta, [UK]), or the number of subscribers (Poland, Cyprus).

For an overview of the different criteria and thresholds in the electricity, gas and oil sector see (NIS Cooperation Group, Sectorial implementation of the NIS Directive in the Energy sector, CG Publication 03/2019, para. 6).

III. Review of the NIS Directive

The review of the NIS Directive concluded that the mixture of approaches led to fragmentation across the Union and thereby confirmed the prior findings of the European Commission in its Report on the consistency of the approaches (COM/2019/546 final, p.84). The Report concludes that the more decentralised the identification system is set up, the more inconsistent is the identification process (ibid). Inconsistencies across the EU are directly linked to two factors: the delegation of the identification process to sectoral authorities and self-identification (ibid, p. 85). Particular challenges arose for OES with cross-border activity in light of the different sizes of Member States and market structures (ibid).

The Commission Report suggested that 'a harmonised set of criteria must be enforced to carry out concretely NIS's mission of a unified increased security maturity within the Single Market' stressing that the importance of a service provider as OES is commonly not limited to one Member State (ibid; see also commentary to Article 5 NIS Directive).

IV. Outlook: The NIS 2 Directive

In order to eliminate the wide divergences among Member States with regard to the criteria to qualify as OES, the NIS 2 Directive establishes a uniform criterion that determines the entities falling within the scope of the NIS 2 Directive and thereby also renders the determination of significant disruptive effect obsolete.

Accordingly, the identification process is abolished and a general size-cap rule is introduced: entities of a type referred to in Annex I or II of the NIS 2 Directive which exceed the ceiling for medium-sized enterprises provided for in Article 2(1) of the Annex to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small, and medium-sized enterprises (OJ [2003] L124/36). This means that all entities of a type referred to in Annex I or II of the NIS 2 Directive that employ at least 50 persons and whose annual turnover and/or annual balance sheet total is at least EUR 10 million will be encompassed. In addition, Member States should also provide for certain small enterprises and microenterprises, as defined in Article 2(2) and (3) of that Annex, which fulfil specific criteria that indicate a key role for society, the economy or for particular sectors or types of service to fall within the scope of this Directive. For an overview of the entities covered by the NIS 2 Directive, see commentary to Article 5 NIS Directive.

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.

I. General Remarks

To achieve and maintain a high level of NIS security, each Member State is required to adopt a national strategy on NIS security (NCSS) defining the strategic objectives and concrete policy actions to be implemented. The obligation to develop and adopt a national strategy is one of the main objectives of the NIS Directive (see also Article 1(2) NIS Directive).

When the Proposal for a NIS Directive was published by the European Commission on 7 February 2013, the majority of Member States had not yet implemented a NCSS. In fact, 18 Member States lacked a national NCSS (Austria, Bulgaria, Croatia, the Czech Republic, Denmark, France, Greece, Hungary, Ireland, Italy, Latvia, Malta, Poland, Portugal, Romania, Slovenia, Spain and Sweden). This, however, does not mean that national policymakers were not addressing NIS security at all. Cybersecurity emerged, for instance, in France already as a policy priority in a White Paper on Defence and National Security published in 2008 (Défense et sécurité nationale: Le Livre Blanc 2008). However, as the French approach shows, NIS security was commonly regarded as a matter for the national defence sector rather than as a comprehensive approach that also addresses civil aspects. In contrast, Germany released a comprehensive NCCS as early as 2011, enhancing national capabilities through the creation of new government agencies and strategic objectives. Distinguishing between defence and civil as well as economic aspects, the strategy responded also to the risks of inter alia industrial espionage and cybercrime.

Already the negotiations on a NIS Directive and the envisaged obligation to adopt a national strategy resulted in most Member States fulfilling the requirement before the NIS Directive entered into force. This was mainly triggered by the forthcoming legal obligation but also by the increased threat landscape. For instance, the impetus for the Czech NCCS was a campaign of cyber attacks targeting Czech media websites, the banking sector and mobile phone operators (Lucie Kadlecová & Michaela Semecká, 'Czech Republic, A new cyber security leader in Central Europe', in: Scott Romaniuk and Mary Manjikian (eds.), *Routledge companion to global cyber-security strategy* (Routledge 2021), p. 52).

When the NIS Directive was finally adopted on 7 July 2016, only four Member States remained without a NCSS: Bulgaria, Bulgaria, Greece, Malta and Sweden. Subsequently, Bulgaria adopted a first NCSS right before the NIS Directive entered into force in August 2016; Malta adopted a first strategy in October 2016, followed by Greece and Sweden, which both adopted their first strategy in 2017. As of June 2023, most Member States have updated their NCSS at least once, see the following timeline of national cybersecurity strategies.

	2009-2012	2013	2014-2015	2016	2017	2018-2019	2020	2021-2023
EU Policy Measure		EU Cybersecurity Strategy 'An Open, Safe and Secure Cyberspace'; Proposal for a NIS Directive		NIS Directive 2016/1148	Renewal of EU Cybersecurity Strategy 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'		EU Cybersecurity Strategy for the Digital Decade; Proposal for a NIS 2 Directive	
Austria		Österreichische Strategie für Cyber Sicherheit July 2013						Österreichische Strategie für Cyber Sicherheit 2021
Belgium	Cyber Security Strategy 2012							Stratégie Cybersecurité Belgique 2.0 2021–2025 2021
Bulgaria				Национална стратегия за киберсигурност „Киберустойчива България 2020" July 2016				Актуализирана Национална стратегия за киберсигурност „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023" 2021
Croatia			Nacionalna Strategija Kiberneti čke Sigurnosti 2015					
Cyprus	Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας 2012						Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας 2020 2020	
Czech Republic			Národní Strategie Kybernetické Bezpe čnosti ČR 2015–2020 2015					Národní Strategie Kybernetické Bezpe čnosti ČR 2021–2025 2021
Denmark			National Strategi for Cyber- og Informationssikkerhed 2015–2016 2014			National Strategi for Cyber- og Informationssikkerhed 2018–2021 2018		National Strategi for Cyber- og Informationssikkerhed 2022–2024 2021
Estonia	Küberjulgeoleku Strateegia 2008–2013 2008		Küberjulgeoleku Strateegia 2014–2017 2014			Küberturvali–suse Strateegia 2019–2022 2019		
Finland		Suomen Kyberturvallisuusstrategia January 2013				Suomen Kyberturvallisuus Strategia 2019		
France			Stratégie Nationale pour la Sécurité du Numérique 2015		Stratégie internationale de la France pour le numérique [complementing the 2015 strategy] 2017			
Germany	Cyber-Sicherheitsstrategie für Deutschland 2011			Cyber-Sicherheitsstrategie für Deutschland November 2016				Cybersicherheitsstrategie für Deutschland 2021

	2009-2012	2013	2014-2015	2016	2017	2018-2019	2020	2021-2023
Greece					ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΑΝΑΘΕ□ΡΗΣΗ 3 2017		ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020-2025 2020	
Hungary		Magyarország Nemzeti Kiberbiztonsági Stratégiájáról June 2013				A hálózati és információs rendszerek biztonságára vonatkozó Stratégia 2018		
Ireland			National Cyber Security Strategy 2015–2017 2015			National Cyber Security Strategy 2019–2024 2019		
Italy		Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico 2013 December 2013			Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica [operational guidelines] 2017			Strategia Nazionale di Cybersicurezza 2022–2026 2022
Latvia			Latvijas Kiberdrošības stratēģija 2014–2018 2014			Latvijas Kiberdrošības stratēģija 2019–2022 2019		Latvijas kiberdrošības stratēģiju 2023–2026 [forthcoming; project stage]
Lithuania	Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinim 2011					Nacionaline Kibernetinio Sugumo Strategija 2018		
Luxembourg	Stratégie Nationale en matière de Cybersécurité 2012		Stratégie Nationale en matière de Cybersécurité II 2015			Stratégie Nationale en matière de Cybersécurité III 2018		Stratégie Nationale en matière de Cybersécurité IV 2021
Malta				Malta Cyber Security Strategy 2016 October 2016				
Netherlands	De Nationale Cyber Security Strategie – Slagkracht door samenwerking 2011		Nationale Cybersecurity Strategie 2 – Van bewust naar bekwaam 2014			Nederlandse Cybersecurity Agenda – Nederland digitaal veilig 2018		Nederlandse Cybersecuritystrategie 2022–2028 – Ambities en acties voor een digitaal veilige samenleving 2022
Poland		Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej 2013 June 2013			Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2017–2022 2017	Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2019–2024 2019		
Portugal			Estratégia Nacional de Segurança do Ciberespaço 2015			Estratégia Nacional de Segurança do Ciberespaço 2019–2023 2019		

	2009-2012	2013	2014-2015	2016	2017	2018-2019	2020	2021-2023
Romania		Strategia de Securitate Cibernetică a României May 2013						Strategia de Securitate Cibernetică a României pentru perioada 2022–2027 2021
Slovakia	Národná stratégia pre informačnú bezpečnosť v Slovenskej republike 2009		Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015–2020 2015					Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 2021
Slovenia				Strategija Kibernetske Varnosti 2016				
Spain		Estrategia de Ciberseguridad Nacional December 2013				Estrategia Nacional de Ciberseguridad 2019		
Sweden					Nationell Strategi för Samhällets Informations- och Cybersäkerhet 2017			

Timeline of national cybersecurity strategies as of June 2023

II. In Detail

Article 7(1) Content of a National Cybersecurity Strategy

A NCSS has to define the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of NIS security of the sectors covered by the NIS Directive.

In that regard, Article 7(1) NIS Directive provides a list of issues that a NCSS should in particular address. According to Article 7(1)(a) NIS Directive, this includes the objectives and priorities of NCSS. A comparison of the objectives listed in national strategies shows that Member States employ different levels of detail. An overview of the objectives of national cybersecurity strategies is provided in the following table.

	AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	GR	HU	IE	IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE
Address cybercrime	x	x	x	x	x	x	x	x	x	x	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x
Adopt information security standards					x	x		x				x		x	x		x						x	x			
Balance security with privacy			x	x	x	x		x	x	x		x		x	x	x						x	x	x	x	x	x
Citizen's awareness		x			x	x	x	x	x	x	x	x		x	x	x	x	x	x		x	x	x	x	x	x	x
Critical information infrastructure protection	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x
Develop national cyber contingency plan	x				x	x	x	x	x	x	x	x	x	x	x	x	x	x			x		x	x		x	x
Engage in international cooperation	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Establish public-private partnership	x	x			x	x		x	x			x		x	x		x	x			x		x	x		x	x
Establish an incident response capability	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Establish an institutiona-	x	x			x	x		x		x	x	x	x	x	x			x			x	x	x	x	x	x	x

lized form of cooperation between public agencies																										
Establish and implement policies and regulation capabilities					x	x					x		x	x		x						x	x			
Establish baseline security requirements	x			x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x		x	
Establish incident reporting mechanism	x	x	x		x	x	x	x	x	x		x	x	x	x			x	x		x	x	x	x	x	x	
Establish trusted information-sharing mechanisms					x	x		x				x		x	x								x	x			
Foster R&D	x	x	x	x	x	x	x	x	x	x	x	x		x	x		x				x	x	x	x		x	x
Improve cybersecurity of supply chain															x								x				
Organise cybersecurity exercises	x	x			x	x	x	x	x	x		x	x	x	x		x	x			x	x	x	x	x	x	x
Provide incentives for the private sector to invest in security measures					x				x			x		x	x								x	x		x	
Risk assessment approach					x	x		x				x		x	x		x						x	x			
Set a clear governance structure					x	x						X		x	x									x			
Strengthen training and educational programmes	x	x	x		x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	

Objectives of national cybersecurity strategies as of June 2023

A NCSS must also include a governance framework to achieve the foreseen objectives and priorities (Article 7(1)(b) NIS Directive). This includes the attribution of respective roles and responsibilities to government bodies and other relevant actors.

Article 7(2) Assistance on the Development of a NCSS

ENISA is tasked to assist Member States on the development of a NCSS.

Article 7(3) Communication to the Commission

Within three months from their adoption, Member States have to communicate their NCSS to the Commission. This obligation does not apply to elements of the NCSS that relate to national security.

III. Review of the NIS Directive

Although all Member States had implemented national strategies, the envisaged level of cybersecurity resilience was still lacking in 2020 due to inter alia the fragmented nature of national strategies and capabilities (European Commission et al., Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665, p. 9). However, the mandatory adoption of NCSS gave impetus to the implementation of further policy actions supporting Member States with less capacity to improve their cybersecurity preparedness and achieve an adequate level of security within their territory (ibid, p. 12).

IV. Outlook: NIS 2 Directive

The NIS 2 Directive is far more specific and detailed on the requirements towards a NCSS. Article 7(1) NIS 2 Directive amends the issues previously encompassed in Article 7(1) NIS Directive and introduces further issues that Member States shall address. This includes enhanced coordination within Member States with regard to the authorities competent under the NIS 2 Directive and those competent under the new CER Directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, [2022] OJ L333/164) in the context of information sharing about risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents, and the exercise of supervisory tasks (Article 7(1)(g) NIS 2 Directive). Further, the NIS 2 Directive requires Member State to include in their NCSS a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens (Article 7(1)(h) NIS 2 Directive).

As part of the NCSS, Member States shall in particular adopt specific policies listed in Article 7(2) NIS 2 Directive. This includes inter alia a policy addressing supply chain security (Article 7(2)(a), and a policy on managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Art 12(1) NIS 2 Directive (Article 7(2)(c) NIS 2 Directive).

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.

I. General Remarks

Articles 1, 3 and 7 NIS Directive foresee the adoption of a national framework by each Member State including a strategy on NIS security as well as regulatory measures covering OESs and DSPs.

The envisaged increase of Member States' capabilities further requires a corresponding institutional setting which is enshrined in Articles 8, 9 and 10 NIS Directive with the designation of a national competent authority (NCA), a single point of contact (SPOC) and at least one computer security incident response team (CSIRT). In that regard, Article 8 NIS Directive requires each Member State to designate at least one national competent authority (NCA) responsible for fulfilling the tasks linked to the security of the NIS of OESs and DSPs under this Directive.

Furthermore, each Member State is required to designate a national single point of contact (SPOC) in order to facilitate cross-border cooperation and communication and to enable effective implementation of the NIS Directive.

II. In Detail

Article 8(1) Designation of a National Competent Authority

Each Member State must designate at least one national competent authority (NCA). Member States may designate more than one authority as NCA in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies (cf. Recital 30 NIS Directive). This shall also avoid duplication.

This approach pays regard to distinctive national governance structures and national specificities. For instance, Luxembourg with its rather large financial market designated the national financial regulatory body Commission de surveillance du secteur financier (CSSF) for the sectors 'credit institutions and financial market infrastructures' as well as the 'digital services provided by an entity falling under the supervision of the CSSF' as NCA under the NIS Directive, while employing a centralised approach for all other DSPs and OESs outside the financial sector. For the latter the Institut luxembourgeois de regulation (ILR) acts as NCA (see Article 3 Loi du 28 mai 2019 portant transposition de la directive(UE) 2016/1148).

The practice in Member States regarding the designation of NCAs is not uniform.

13 Member States (Bulgaria, Croatia, Czech Republic, Denmark, Finland, Hungary, Italy, Latvia, Luxembourg, the Netherlands, Poland, Spain and Sweden) designated more than one NCA, employing a decentralised approach. In most cases existing sector-specific authorities have been assigned the task of NCA under the NIS Directive.

14 Member States (Austria, Belgium, Cyprus, Estonia, France, Germany, Greece, Ireland, Lithuania, Malta, Portugal, Romania, Slovakia and Slovenia) opted for a centralised approach with a single NCA for DSPs and OESs which at the same time serves as SPOC. The centralised approach allows the NCA to have more control over the information disclosed by OESs and DSPs. Further this approach may encourage the NCA to take the lead in cross-border cooperation. With the bundling of skills and pooling of expertise, they may also be more active in cross-border cooperation and the NIS CG.

Article 8(2) Tasks of the NCAs

NCAs have to monitor the application of the NIS Directive at national level. In that regard, the NIS Directive specifies a number of tasks in its operative part.

According to Article 10(2) NIS Directive, incident notifications pursuant to Articles 14(3) and 16(3) must be submitted to the NCAs or the CSIRTs depending which entity has been assigned this competence. The notification recipient then bears a coordinating role (see Articles 14(3) to (7) and 16(3) to (7) NIS Directive); for instance other Member State(s) have to be informed if they are affected and the SPOC may be requested to forward notifications to the SPOCs in other Member States (Articles 14(5) and 16(6) NIS Directive).

The NCAs have to assess the compliance of OESs (Article 15 NIS Directive) and DSPs (Article 17 NIS Directive), and must thus be equipped with the respective powers. Member States must ensure that NCAs have the powers to carry out security audits and issue binding instructions to the entities concerned to remedy the deficiencies identified (Articles 15(2) and 17(2) NIS Directive).

Article 8(3) Designation of a SPOC

In order to facilitate cross-border cooperation and communication, Member States shall designate a national SPOC.

Article 8(3) of the Directive specifies if a Member State adopts a centralised approach and designates only one competent authority, that competent authority shall also be the SPOC. Where a Member State adopts a decentralised approach, i.e. designates more than one NCA, one of these different NCAs may act as SPOC. This is for instance the case in Finland, where sectoral authorities have been designated as NCAs, with the National Cyber Security Centre at the Finnish Transport and Communications Agency acting as SPOC. However, it is not required that a designated NCA also serves as SPOC. Where more than one NCA exists, the task of SPOC has also been assigned to a separate agency. For instance, in Bulgaria, the state E-Government Agency serves as SPOC without having the status of a NCA.

Whenever the competent authority and SPOC are separate entities, Article 10 NIS Directive requires that Member States ensure effective cooperation among them.

Article 8(4) Tasks of the SPOC

The SPOC is responsible for coordinating issues related to NIS security and cross-border cooperation at EU level. This includes a liaison function to ensure cross-border cooperation of Member State authorities, the NIS CG and the CSIRTs network.

In contrast to NCAs or CSIRTs, SPOCs should not receive incident notifications directly – unless they also act as the authority competent to receive notifications.

In consideration of their role in cross-border cooperation and coordination, SPOCs can be tasked by the NCA or a CSIRT to forward incident notifications to the SPOCs of other affected Member States (see Article 14(5)).

The SPOC is responsible for submitting a summary report on notified incidents to the NIS CG (see Article 10(3)). In that regard, the Member States must ensure that the NCAs or the CSIRTs inform the SPOC about incident notifications that they have received (see ibid and Recital 32). The SPOC than has to anonymise the information in the report to preserve the confidentiality of the notifications and the identity of OES and DPSs, as information on the identity of the notifying entities is not required for the exchange of best practice in the NIS CG. 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 type of security breaches, their seriousness or their duration.

Article 8(5) Resources of NCAs and SPOCs to Carry out Assigned Tasks

NCAs and SPOCs must 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 the NIS Directive (Recital 31 NIS Directive). As the NIS 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 (ibid).

Member States must also ensure effective, efficient and secure cooperation of the designated representatives in the NIS CG.

Article 8(6) Cooperation with Law Enforcement Authorities and National Data Protection Authorities

NCAs and SPOCs shall consult and cooperate with national law enforcement authorities (LEA) and DPAs whenever appropriate and in accordance with national law.

Since incidents may be the result of criminal activities, investigation and prosecution should be supported by NCAs (see Recital 62 NIS Directive).

When incidents result in data breaches, Article 15(4) NIS Directive foresees that NCAs shall work in close cooperation with DPAs when addressing these kind of incidents. Recital 63 NIS Directive briefly addresses this cooperation, noting that, NCAs and DPAs shall cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents (see Recital 63 NIS Directive).

Article 8(7) Notification of Commission as regards Designation of NCAs and SPOCs

Member States are obliged to immediately notify the Commission the designation of the NCA(s) and SPOC and any subsequent changes thereto. The notification must also contain information about their tasks. Further the designation of the NCA(s) and SPOC has to be made public. The Commission must publish the list of designated SPOCs. A list of SPOCS

and competent authorities has been published on the website dedicated to the NIS CG. The following list has been amended to include the contact details of the respective NCAs, CSIRTs and SPOCs.

Country	Single Point of Contact	Competent Authority for DSPs	Competent Authority for OES	National CSIRT
Austria	Federal Ministry of the Interior – *Bundesministerium für Inneres*	Federal Chancellery of Austria – *Bundeskanzleramt* *Federal Ministry of the Interior*	Same as previous	For OES and DSP: CERT.at For public administration GovCERT Austria
Belgium	Center for Cybersecurity – *Centre pour la Cybersécurité Belgique (CCB)*	Same as previous	Same as previous	Cert.be operated by *Center for Cybersecurity Belgium*
Bulgaria	State "E-gov" Agency - *Държавна агенция "Електронно управление"*	/	/	National CERT.bg
Croatia	Office of the National Security Council – Ureda Vijeća za nacionalnu sigurnost	Ministry of Economy and Sustainable Development – Ministarstvo gospodarstva i održivog razvoja	**Energy** (All sub-ectors) Ministry of Environment and Energy – Ministarstvo gospodarstva i održivog razvoja **Transport** Ministry of the Sea, Transport and infrastructure – Ministarstvo mora, prometa i infrastrukture **Banking** Croatian National Bank – Hrvatska Narodna Banka **Financial market infrastructures** Croatian Financial Services Supervisory Agency – *Hrvatska agencija za nadzor financijskih usluga* **Health sector** Ministry of Health – Ministarstvo zdravstva **Drinking water supply and distribution** Ministry of Environment and Energy - Ministarstvo gospodarstva i održivog razvoja **Digital infrastructure** Central State Office for the Development of the Digital Society	For Banking, Financial market infrastructures, Digital infrastructure, DSPs and Information Systems: National CERT For Energy, Transport, Health sector, Drinking water supply and distribution: Security Bureau
Cyprus	Digital Security Authority (DSA)	/	/	National CSIRT (CSIRT.cy)
Czech Republic	National cyber and information security agency – Národní úřad pro kybernetickou a informační bezpečnost	CZ Domain registry – CZ NIC	Same as previous	**For OES:** GovCERT operated by National cyber and information security agency **For DSPs:** CSIRT.CZ operated by CZ.NIC
Denmark	Danish Center for Cybersecurity – Center for Cybersikkerheid	Danish Business Authority – Erhvervsstyrelsen	**Energy (All sub-sectors)** Danish Energy Agency – Energistyrelsen Transport (All sub-sectors) The Danish Transport, Construction and Housing Authority – Trafik-, Bygge- og Boligstyrelsen	Same as single point of contact.

			Transport (Maritime) The Danish Maritime Authority – Søfartsstyrelsen **Banking and financial market infrastructures** Danish Financial Supervisory Authority - Finanstilsynet **Health sector** The Danish Health Data Authority – Sundhedsstyrelsen **Drinking water supply and distribution** Ministry of Environment and Food - Ministeriet for Fødevarer, Landbrug og Fiskeri	
Estonia	Estonian Information System Authority – Riigi infosüsteem Amet	Same as previous	Same as previous	Estonian Information System Authority
Finland	National Cyber Security Centre – Kyberturvallisuuskeskus	Same as previous	**Energy (All sub-sectors)** Energy Authority – energiavirasto **Transport (All sub-sectors)** Finnish Transport Safety Agency – Liikenne- ja viestintävirasto Traficom **Banking and Financial market infrastructures** Financial Supervisory Authority – Finanssivalvonta **Health sector** National Supervisory Authority for Welfare and Health – Valvira **Drinking water supply and distribution** Centre for Economic Development, Transport and the Environment – Elinkeino-, liikenne- ja ympäristökeskus **Digital infrastructure** Finnish Communications Regulatory Authority – Liikenne- ja viestintävirasto Traficom	Same as single point of contact
France	Agence national de la sécurité des systèmes de l'information (ANSSI)	Same as previous	/	CERT-FR
Germany	Federal Office for Information Security – *Bundesamt für Sicherheit in der Informationstechnik*	Same as previous	Same as previous	Same as previous
Greece	National Cyber Security Authority (General Secretariat of Digital Policy – Ministry of Digital Policy, Telecommunications and Media) - Γενική Διεύθυνση Κυβερνοασφάλειας	Same as previous	Same as previous	National Authority Against Electronic Attacks – National Cert
Hungary	Nation Cyber Security Center – Nemzeti Kibervédelmi Intézet	Same as previous	National Directorate General for Disaster Management – *Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság*	CSIRT@nki.gov.hu
Ireland	The National Cyber Security Centre (NCSC)	Department of Communications, Climate Action & Environment	Same as previous	Same as single point of contact

Italy	Presidenza del Consiglio dei Ministri - DIS	Ministero dello Sviluppo Economico - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI)	**Energy** Ministero dello Sviluppo Economico - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) **Transport** Ministero delle Infrastrutture e dei Trasporti - Organo Centrale di Sicurezza **Banking and financial market** infrastructures Ministero dell'Economia e delle Finanze **Health sector** Ministero della Salute **Drinking water supply and distribution** Ministero dell'ambiente e della tutela del territorio e del mare **Digital infrastructure** Ministero dello Sviluppo Economico - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI)	/
Latvia	Minstery of Defence – Aizsardzības ministrija	Ministry of Transport – Lietuvos Respublikos susisiekimo ministerija	**Energy** Ministry of Economics – *Ekonomikas ministrija* **Transport** (All sub-sectors) Ministry of Transport – Satiksmes ministrija **Banking and financial market infrastructure** Financial and Capital Market Commission – *Finanšu un kapitāla tirgus komisija* **Health sector** Ministry of Health – *Veselības ministrija* **Drinking water supply and distribution** Ministry of Health (MoH) and the Ministry of Agriculture (MoA) - *Zemkopības ministrija* **Digital infrastructure** Ministry of Transport – *Satiksmes ministrija*	Information Technology Security Incident Response Institution CERT.LV.
Lithuania	National Cyber Security Centre (NCSC/CERT-LT) – Nacionalinis Kibernetinio Saugumo Centras	Same as previous	Same as previous	Same as previous
Luxembourg	Institut Luxembourgeois de Régulation	Same as previous	**Banking and financial market infrastructures** Commission de Surveillance du Secteur Financier **For all other sectors:** Same as single point of contact	National CSIRT CERT Gouvernemental / CERT National
Malta	Critical Information Infrastructure Protection Unit	Same as previous	Same as previous	CSIRTMalta
Netherlands	NCSC – Nationaal Cyber Security Centrum	Radio Communications Agency – Agentschap Telecom	**Energy (All sub-sectors)** Agentschap Telecom	Ministry of Economic Affairs and Climate

			Banking and financial market infrastructure De Nederlandsche Bank (DNB) **Health sector** Inspectorate Healthcare and Youth – *Inspectie Gezondheidszorg en Jeugd* **Drinking water supply and distribution** Ministry of Infrastructure and Water Management – *Ministerie van Infrastructuur en Waterstaat* **Digital infrastructure** Agentschap Telecom	
Poland	Ministry of Digital Affairs - Department of Cybersecurity - *Cyfryzacja KPRM*	Same as previous + Ministry of National Defence of the Republic of Poland	**Energy** Ministry of Climate – *Ministerstwo Klimatu i Środowiska* **Transport** Ministry of Infrastructure – *Ministerstwo Infrastruktury* **Transport (only for water transport sub-sector)** Ministry of Marine Economy and Inland Navigation – *Archiwalna strona Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej* **Banking and financial markets infrastructure** Polish Financial Supervision Authority – *Komisja Nadzoru Finansowego* **Health sector** Ministry of Health – *Ministerstwo Zdrowia* + Ministry of National Defence of the Republic of Poland – *Ministerstwo Obrony Narodowe* **Drinking water supply and distribution** Ministry of Marine Economy and Inland Navigation – *Archiwalna strona Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej* **Digital Infrastructure** Ministry of Digital Affairs – *Ministerstwo Cyfryzacji* **Digital Infrastructure** Ministry of National Defence of the Republic of Poland – *Ministerstwo Obrony Narodowe*	CSIRT GOV
Portugal	Portuguese National Cybersecurity Centre – Centro Nacional de Cibersegurança	Same as previous	Same as previous	CERT.PT
Romania	Romanian National Computer Security Incident Response Team (CERT.ro) – Centrul National de	Same as previous	Same as previous	Same as previous

	Răspuns la Incidente de Securitate Cibernetică			
Slovakia	National Security Authority – Národný bezpečnostný úrad			National SK - CERT
Slovenia	Information Security Administration – Uprava Republike Slovenije za informacijsko varnost	Same as previous	Same as previous	Slovenian National Cyber Security Incident Response Centre
Spain	National Security Council, through the National Security Department – Departamento de Seguridad Nacional	**For private sector:** Secretary of State for Information Society and Digital Agenda – Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales **For public sector:** Ministry of the Presidency and for the Territorial Administrations, through the National Cryptologic Centre – Ministerio de Política Territorial y Función Pública	National Center for the Protection of Infrastructures and Cybersecurity (CNPIC) – Centro Nacional de Protección de Infraestructuras y Ciberseguridad	**Private sector** INCIBE-CERT, National Cybersecurity Institute **Public sector** CCN-CERT, National Cryptologic Centre
Sweden	Myndigheten för samhällsskydd och beredskap - MSB	Post- och telestyrelsen	**Energy (All sub-sectors)** Energimyndigheten **Transport (All sub-sectors)** Transportstyrelsen **Banking and financial market infrastructures** Finansinspektionen **Health sector** Inspektionen för vård och omsorg **Drinking water supply and distribution** Livsmedelsverket	MSB/CERT-SE

Overview national NCAs, CSIRTs and SPOCs including contact details as of May 2022.

III. Review of the NIS Directive

The variety of NCAs posed a challenge for cross-border cooperation. Although NCAs report that cooperation improved with the NIS Directive (see EnCaViBS, Summary Report on Cooperation), there are claims that the existence of a variety of NCAs made it difficult for public sector bodies to identify their counterparts with whom to relate in other Member States.

During the review of the Directive, a shortcoming related to the implementation of the NIS directive was the remaining insufficient exchange of information and cooperation among Member States. This shortcoming was inter alia blamed on the lack of clarity on who is responsible for cross-border cooperation (see European Commission et al., Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665 p. 13). In fact, the challenge to identify whether the SPOC or a CSIRT within a Member State is responsible for cross-border cooperation was identified as one of the main challenges faced in cooperation.

The interviews conducted in the course of the Study to support the NIS Directive Review also revealed that inadequate financial and human resources are one of the most relevant challenges that NCAs have faced in the implementation of the Directive (ibid, p. 27). Accordingly, the fitness of operational capacity and reliability of national CSIRTs greatly

varies (ibid, p. 32). This may also contribute to a varying level of cooperation with national LEA, SPOCs and judicial and other competent authorities (ibid).

The stakeholders involved in the aforementioned study raised concerns that the tasks attributed to SPOCs at national level are sometimes overlapping with those of the CSIRTs, stressing that the liaison function of SPOCs should be further clarified (ibid, p. 27). It has also been argued that SPOCs should be given more responsibilities other than just forwarding information between different stakeholders.

As regards the effectiveness of CSIRTs, the expectations of the stakeholders with regard to the provision of a dynamic risk and incident analysis and situational awareness as well as the promotion of the adoption and use of common or standardised practices for incident and risk-handling procedures have not been fulfilled (ibid). Challenges addressed by OESs relate to the lack of understanding by CSIRTs of their particular field of activity, a lack of support for the private sector in sharing information, and a lack of systematic directive to CSIRts to share information with established private sector initiatives (ibid). In sum, the institutional setting as outlined did not provide for an increase in trusted information sharing between the private and public sector.

IV. Outlook: The NIS 2 Directive

The rules on the establishment of NCAs and SPOCs can be found in Article 8 NIS 2 Directive. Article 8 NIS 2 Directive is almost identical to Article 8 NIS Directive. Article 8(4) has been amended to clarify the liaison function of SPOCs as to include, where appropriate, liaising with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other NCAs within its Member State.

As regards an extension of tasks of CSIRTs, these will be addressed in the respective articles. At this point, it shall only be highlighted that the addressee of incident notifications has been attributed a far more active role than under the NIS Directive where the role was rather passive at the receiving end.

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.

I. General Remarks

The envisaged increase of Member States' capabilities requires a corresponding institutional setting which is enshrined in Articles 8, 9 and 10 NIS Directive with the designation of a national competent authority (NCA), a single point of contact (SPOC) and at least one computer security incident response team (CSIRT).

In that regard, Article 9 NIS Directive sets forth that each Member State shall designate at least one CSIRT responsible for risk and incident handling.

II. In Detail

Article 9(1) Designation of CSIRT(s)

Each Member State must designate at least one computer security incident response team (CSIRT). The CSIRT may be established within a competent authority. This approach has for instance been taken in Belgium, Bulgaria, Cyprus and Germany.

The Member States must ensure that the CSIRTs function well and comply with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level (Recital 24 NIS Directive). In order for

all types of OESs and DSPs to benefit from such capabilities and cooperation, the CSIRT must comply with the requirements set out in point (1) of Annex I, covering at least the sectors of Annex II in which the OES are active, and the services referred to in Annex III, which sets out the types of digital services covered by the NIS Directive.

Point (1) of Annex I contains a non-exhaustive list of the requirements and tasks of CSIRTs that shall be adequately and clearly defined and be supported by national policy and/or regulation. 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 (Point (1)(a) Annex I). As regards the premises and the supporting information systems, these shall be located in secure sites ((Point (1)(b) Annex I).

To carry out their tasks, business continuity of CSIRTs is key. In order to guarantee business continuity, CSIRTs shall be equipped with an appropriate system for managing and routing requests in order to facilitate handovers, they shall be adequately staffed to ensure availability at all times, and rely on an infrastructure of which the continuity is ensured – to that end, redundant systems and backup working space shall be available (Point (1)(c) Annex I). CSIRTs shall also have the possibility to participate, where they wish to do so, in international cooperation networks ((Point (1)(d) Annex I). On a global level, exists for instance the Forum for Incident Response and Security Teams (FIRST), which was founded in the U.S. in 1990 with the mission of improving information sharing and assisting in the coordination of CSIRTs during network-wide incidents. Further international cooperation networks include the International Watch and Warning Network (IWWN), of which for instance the Dutch and the German CSIRT are members; and the Global Forum on Cyber Expertise (GFCE), which is a forum for sharing best practices and expertise internationally.

The incident and risk-handling procedure at the CSIRT must be in accordance with a well-defined process, for which no further guidance is provided in the NIS Directive.

Article 9(2) Attribution of Adequate Resources and Cooperation in the CSIRTs Network

CSIRTs provide a range of services. The tasks required by the NIS Directive are set out in Point (2) Annex I and 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 (Point (2)(a) Annex I).

In addition, CSIRTs shall establish cooperation relationships with the private sector (Point (2)(b) Annex I). In this regard, for instance, in the Netherlands the ICT Response Board (IRB) has been established as a public-private board in which representatives of vital infrastructure organisations analyse the situation and give an advice to the national

decision-making structure. The most common forum for cooperation relationships with the private sector are however Information Sharing and Analysis Centers (ISACs) with industry organisations.

In order 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 (Point (2)(c) Annex I).

Furthermore, Member States are required to ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12. The creation of the CSIRTs network seeks to enable Member States to ensure effective cooperation and participation in exercises (see comment on Article 12 NIS Directive).

Article 9(3) Access to Appropriate, Secure and Resilient Communication and Information Infrastructure

Member States are required to ensure that their national CSIRT(s) have access to an appropriate, secure, and resilient communication and information infrastructure at national level. This includes security of the NIS used by CSIRTs, but also security of their premises. In terms of resilience, 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 (Point (1)(a) Annex I). As regards the premises and the supporting information systems, these shall be located in secure sites ((Point (1)(b) Annex I).

Article 9(4) Obligation to Inform the Commission

When Member States are required to inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs, this regards the national procedure in general.

Article 9(5) Assistance by ENISA for the Development of National CSIRTs

In application of the NIS Directive, ENISA fulfils a consulting role (cf. Recital 36 NIS Directive). Member States should be able to consult ENISA in any matter relating to the application of the Directive; this includes assistance in developing national CSIRTs. This assistance consists of advice and guidance.

III. Review of the NIS Directive

In the context of CSIRTs, it is necessary to address, that there are many more CSIRTs in Europe than those designated under the NIS Directive. Thus, if for instance, the Study to support the NIS Review states that 'all Member States have set up one or more national and/or government CSIRT' (see European Commission et al., Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665,

p. 13), it must be emphasized that government CSIRTs are not founded in the NIS Directive. Accordingly, the number of '464 CSIRTs declared to ENISA' also includes CSIRTs in sectors outside the scope of the Directive.

The Study to support the review of the NIS Directive identified that there is a practical need to improve the information-sharing within and between CSIRTs. Although the designation of national CSIRTs has been welcomed, in practice a number of flaws could be revealed: OESs complained that when cooperating not only with the NCAs but also with the national CSIRTs, they were confronted with a lack of understanding about their field of activity, the focus on national critical infrastructure rather than cross-border dependencies, and a lack of support for information sharing, such as a mechanism for CSIRTs and National Cyber Security Centres (NCSCs) to share information with established private sector initiatives under public private partnership programmes (ibid, pp. 13 and 27). In terms of cross-border cooperation, he stakeholders involved in the aforementioned study raised concerns that the tasks attributed to SPOCs at national level are sometimes overlapping with those of the CSIRTs, stressing that the liaison function of SPOCs should be further clarified (ibid, p. 27). Also, a lack of clarity in terms of responsibility could be identified, meaning that Member States had been struggling to identify whether the SPOC or the CSIRT within a certain Member States should be addressed (ibid, p. 13). The fitness of operational capacity and reliability of national CSIRTs also varies (ibid, p. 32).

During the review, there was strong support from the stakeholders involved to strengthen the role of CSIRTs by introducing new tasks and responsibilities for them. In sum, the institutional setting as outlined did not provide for an increase in trusted information sharing between the private and public sector.

IV. Outlook: The NIS 2 Directive

The role of the CSIRTs is strengthened in comparison to the NIS Directive. While the tasks and requirements of the CSIRTs have been enlisted in an Annex to the NIS Directive, these have now been placed in the operative part within Article 11 NIS 2 Directive. In addition, Article 10 NIS 2 Directive now contains the general rules on designation or establishments of CSIRTs formerly enshrined in Article 9 NIS Directive. A new section 3 seeks to ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders.

The NIS 2 Directive responds to the divergences in the operational fitness of CSIRTs. In that regard, CSIRTs must be prepared to handle large volumes of sometimes sensitive data (Recital 42). Accordingly, the infrastructure as well as the staff must have the resources to ensure the confidentiality and trustworthiness of their operations (ibid). In terms of fitness of national CSIRTs, Article 11(1) and (2) NIS 2 Directive stresses that Member States must

ensure that the CSIRTs have adequate resources and technical capabilities. In order to enhance the trust relationship between the entities covered and the CSIRTs, where a CSIRT is part of a NCA, Member States should consider a functional separation between the operational tasks provided by the CSIRTs (in particular concerning information sharing), the provision of assistance to the entities, and the supervisory activities of the NCAs (Recital 41).

In view of new and/or extended tasks and responsibilities of the CSIRTs as well as the estimated tremendous increase in entities covered (the increase of entities is estimated up to forty-fold, see for instance Pieter Byttebier, NIS-2: Where are you?), it is obvious that all Member States have to increase the level of resources of NCAs and CSIRTs alike.

The tasks of the CSIRTs are now enlisted under Article 11(3) NIS 2 Directive, but further also include the establishment of and cooperation in voluntary cooperation frameworks with third countries (Article 10(7) and (8) NIS 2 Directive). An overview of the tasks under Article 11(3) NIS 2 Directive compared to the prior tasks under point (2) Annex I NIS Directive is provided in the following table.

Art. 11(3) NIS 2 Directive	Point (2) Annex I NIS 1 Directive
(a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;	(i) monitoring incidents at a national level;
(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;	(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable	(iii) responding to incidents;
(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(iv) providing dynamic risk and incident analysis and situational awareness;
(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;	
(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;	(v) participating in the CSIRTs network.

(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);	
(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).	

Overview tasks of a CSIRT under NIS 2 Directive and NIS Directive

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.

I. General Remarks

In order to increase the common level of NIS security, Member States are required to improve their cooperation with each other.

Before the NIS Directive entered into force, a low level of protection in many Member States constituted an obstacle for cooperation and information sharing: information sharing is a matter of trust and insufficient protection hinders the creation of trust among peers (see Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM/2013/048 final, Explanatory memorandum, para. 1.1). The Explanatory Memorandum to the Proposal for a NIS Directive thus stated that cooperation was limited to those Member States with a high level of capabilities (ibid). Accordingly, cooperation and information sharing appeared underdeveloped and were limited to informal information exchange or cooperation schemes between Member States. In 2013, when the Proposal for a NIS Directive

was published, an effective mechanism at EU level for effective cooperation and collaboration and for trusted information sharing on NIS incidents and risks among Member States was lacking (ibid). As a consequence, there was a risk of uncoordinated regulatory interventions, incoherent strategies and divergent standards, which in turn led to insufficient protection of NIS security (ibid). The European Commission recognized the need for a network of NCAs in order to enable secure and effective coordination 'including coordinated information exchange as well as detection and response at EU level' (ibid).

The idea of an integrated EU approach tackling the security and resilience of NIS at EU level had previously inter alia been addressed in the Commission Communication on Critical Information Infrastructure Protection (COM/2009/149 final) and the Council Resolution on a collaborative European Approach to Network and Information Security ([2009] OJ C321/1) in 2009; both interventions must be seen as direct responses to the large-scale cyber-attacks targeting Estonia in 2007 and the unprecedented level of sophistication of cyber-attacks in general, while dependence on critical infrastructure was on the rise. The Digital Agenda for Europe (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2010/0245 final) and the Council Conclusions on the Agenda of May 2010 also stressed the need for cooperation mechanisms and a system of contact points to respond to cyber threats.

In order to eliminate differences in national approaches and to tackle the lack of systematic cross-border cooperation, the NIS Directive introduces several multi-stakeholder and multi-level approaches for cooperation: (1) Article 11 NIS Directive establishes the NIS Cooperation Group (NIS CG) which is composed of representatives of the Member States, the Commission and ENISA; Article 12 NIS Directive establishes a network of national computer security incident response teams (CSIRTs network); Article 13 NIS Directive provides a legal basis for the EU to conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the NISCG. Besides these cooperation mechanisms among Member States, Article 10 NIS Directive also requires effective cooperation between the relevant actors at national level.

II. In Detail

Article 11(1) - (3) NIS Cooperation Group: Composition and Tasks

1. Composition of the NIS Cooperation Group

In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, the NIS Cooperation Group (NIS CG) was established under Article 11 NIS Directive.

According to Article 11(2) NIS Directive, the NIS CG is composed of representatives of the Member States, the Commission and the EU Agency for Cybersecurity (ENISA). If appropriate, the NIS CG may invite representatives of the relevant stakeholders to

participate in its work (Article 11(2) NIS Directive). Relevant stakeholders include countries that are acceding the EU from the date of signature of the Treaty of accession. Their presence shall ensure that they comply with the requirements of the NIS Directive from the day of accession (cf. Article 7(1) Commission Implementing Decision (EU) 2017/179, [2017] OJ L28/73). Furthermore, the NIS CG may invite DSPs or OESs to participate in information exchange (Recital 35 NIS Directive). Besides relevant stakeholders, Article 7(2) of Commission Implementing Decision (EU) 2017/179 foresees the participation of invited experts in a meeting or in a particular part of a meeting. Third parties further include third countries and international organisations with whom the EU has concluded international cooperation agreements in accordance with Article 13 NIS Directive, that allow and organize their participation in some activities of the NIS CG (ibid). Representatives of third parties, relevant stakeholders and experts are excluded from attending or participating in voting of the NIS CG (Article 7(3) Commission Implementing Decision (EU) 2017/179).

2. The NIS Cooperation Group Secretariat

Pursuant to Article 11(2) NIS Directive, the secretariat of the NIS CG is provided by the European Commission. This also includes secretarial support for sub-groups created in accordance with Commission Implementing Decision (EU) 2017/179 (see Article 8(3) of this Decision).

3. The Chair of the NIS Cooperation Group

The chairmanship is filled by a representative of the Member State holding the Presidency of the Council of the EU (Article 2(1) Commission Implementing Decision (EU) 2017/179, [2017] OJ L28/73). In order to ensure continuity in the work of the NIS CG, the procedural arrangements of the NIS CG foresee that the Chair is assisted in the performance of his duties by representatives of the Member States holding the previous and the following Presidency of the Council of the Union (ibid). If the Member State holding the Presidency of the Council refrains from chairing the NIS CG, the NIS CG may decide by a two-third majority to elect a substitute chair (Article 2(2) Commission Implementing Decision (EU) 2017/179, [2017] OJ L28/73). The Chair's tasks includes convening meetings (Article 3 Commission Implementing Decision (EU) 2017/179), drawing up the meeting agenda (Article 5 Commission Implementing Decision (EU) 2017/179), deciding to invite representatives of relevant stakeholders or experts to participate in meetings (Article 7 Commission Implementing Decision (EU) 2017/179), the proposition of amendments to the rules of procedure (Article 9(2) Commission Implementing Decision (EU) 2017/179), and ensuring that representatives of third parties and experts are made aware of the confidentiality requirements imposed upon them (Article 10(5) Commission Implementing Decision (EU) 2017/179).

4. Tasks of the NIS Cooperation Group

Article 11(3) NIS Directive enlists the tasks of the NIS CG; these include inter alia the provision of strategic guidance for the activities of the CSIRTs network, the exchange of

information and best practice between Member States (for instance on best practice in relation to the information exchange related to incident reports by OESs and DSPs), discussing capabilities and preparedness of member States. Further, the NIS CG serves as a discussion forum for incident reporting modalities, OES identification, and best practices for information exchange related to incident reports with a cross-border element.

The NIS CG is required to cooperate with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practice, and to provide advice on NIS security aspects that might have an impact on their work (Recital 39 NIS Directive).

Pursuant to Article 11(3)(j) NIS Directive, the NIS CG examines on an annual basis the summary reports on notifications received which are provided by the national SPOCs under Article 10(3) NIS Directive.

The tasks of the NIS CG and ENISA are interdependent and complementary; ENISA should assist the NIS CG in the execution of its tasks (Recital 38 NIS Directive).

In order to carry out its tasks, the NIS CG meets four times per annum. The meeting agendas are published by the European Commission on a dedicated website. At this meetings, the NIS CG also adopts its biennial work programmes as required by Article 11(1) NIS Directive.

The NIS CG is required to carry out its tasks on the basis of these biennial work programmes; the first programme for 2018-2019 had to be established by 9 February 2018. The second work programme (2018-2020) was adopted in the course of the NIS CG meeting on 28 January 2020 (NIS CG, 14th Meeting of the NIS CG, Agenda). The strategic goals of third biennial work programme have been discussed in the NIS CG meeting on 10 February 2022 (NIS CG, 22nd Meeting of the NIS CG, Agenda). These goals are: facilitating the implementation of the NIS 2 Directive, strategic discussions on key policy files for cybersecurity in the EU, and the operationalizing of sharing of information and best practices. Further the NIS CG proposes a new focus of work streams on large scale cyber incidents and crises and supply chain security; both these elements are part of the Proposal for a NIS 2 Directive.

The biennial work programmes have not been opened to the public. In principle, the discussions of the NIS CG should not be open to the public in order to avoid negative implications for trust and confidence building between the members and in consideration of the fact that matters discussed often concern public security (Recital 13 and Article 10 Commission Implementing Decision (EU) 2017/179, [2017] OJ L28/73). In agreement with the Chair, the NIS CG may decide to open up its discussions to the public restricted to certain subject matters (Article 10(2) Commission Implementing Decision (EU) 2017/179).

Article 11(4) NIS Cooperation Group Report

The NIS CG is also required to prepare by 9 August 2018 and every year and half thereafter, a report assessing the experience gained with the strategic cooperation pursued under this Article. The first report was presented on 10 October 2018 at the 8th NIS CG meeting, the second

report on 28 January 2020 at the 14th NIS CG meeting, and the third report was adopted on 10 February 2022 during the 22th NIS CG meeting.

Article 11(5) Implementing Acts

Implementing powers have been conferred on the Commission to lay down the procedural arrangements necessary for the smooth functioning of the Group. These procedural arrangements have been laid down in an implementing act: the Commission Implementing Decision (EU) 2017/179, [2017] OJ L28/73 of 1 February 2017. In accordance with Article 9(1) of the Commission Implementing Decision (EU) 2017/179, the NIS CG adopted its own rules of procedure during its first official NIS CG meeting on 9 February 2017.

III. Review of the NIS Directive

The review of the NIS Directive appreciated the flexibility of the NIS CG since the flexible forum allowed to react to changing and new policy priorities and challenges. Stakeholders also valued the contribution of this forum to an increase in information exchange (see EnCaViBS, Summary Report on Cooperation). The NIS CG plays a key role in facilitating cooperation and exchange of information among Member States through its meetings, pieces of training, and reference documents (European Commission et al., Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665, p. 28). Further the NIS CG was effective in assisting Member States, exchanging best practices, and providing initiatives including education programmes and training (ibid). However, despite the effectiveness of the NIS CG in assisting Member States in capacity building and information exchange, and the establishment of the CSIRTs network, the envisaged swift and effective operational cross-border cooperation has not been fully achieved (ibid, p. 13). Although the NIS CG is not the forum to set the parameter for effective operational cross-border cooperation, the study partly blames the NIS CG for limited cooperation.

IV. Outlook: The NIS 2 Directive

Under the NIS 2 Directive the NIS CG remains a flexible forum with the ability to reach to changing and new policy priorities and to tackle new challenges (see Recital 66 NIS 2 Directive). Regular joint meetings with relevant private stakeholders are encouraged. In order to enhance cooperation at EU level, the NIS CG should also consider inviting relevant Union institutions, bodies, offices and agencies involved in cybersecurity policy, such as the European Parliament, Europol, the European Data Protection Board, the European Union Aviation Safety Agency, and the European Union Agency for Space Programme to participate in its work (Article 14(3) NIS 2 Directive).

The list of tasks for the NIS CG has been extended under Article 14(4) NIS 2 Directive and the tasks are more precise and detailed than previously under Article 11(3) NIS Directive.

New tasks of the NIS CG include the establishment of a self-assessment methodology for Member States aiming to cover factors such as the level of implementation of the cybersecurity risk-management measures and reporting obligations, the level of capabilities and the effectiveness of the exercise of the tasks of the competent national authorities, the operational capabilities of the CSIRTs, the level of implementation of mutual assistance, the level of implementation of the cybersecurity information sharing arrangements, or specific issues of cross-border or cross-sector nature (Recital 76; Article 14(4)(q) NIS 2 Directive). Member States should be encouraged to carry out the self-assessment on a regular basis, and present and discuss their results within the NIS CG (ibid).

With the study to support the review of the NIS Directive suggesting that a more structured cooperation between the NIS CG and the CSIRTs network could be beneficial (ibid, p. 28), the NIS 2 Directive sets up a cooperation framework with regard to strategic guidance by the NIS CG to the CSIRTs network on specific emerging issues (Article 14(4)(l) NIS 2 Directive), and a mandatory exchange of views on the policy on follow-up actions following large-scale cybersecurity incidents and crisis (Article 14(4)(m) NIS 2 Directive). Furthermore, the NIS CG is tasked to facilitate the exchange of national officials through a capacity building programme involving staff also from the CSIRTs network (Article 14(4)(n) NIS 2 Directive). Finally, the NIS CG may rely on the expertise of CSIRTs by requesting from the CSIRTs network technical reports on selected topics (Article 14(6) NIS 2 Directive).

The NIS 2 Directive also provides for a more structured approach of the NIS CG towards its deliverables. For instance the tasks are no longer more or less restricted to discussing, exchanging or collecting information but, to draw up conclusions and recommendations, as well as to carry out coordinated assessments. In that regard, recital 65 NIS 2 Directive notes that when developing guidance documents, the NIS CG should consistently map national solutions and experiences, assess the impact of their deliverables on national approaches, discuss implementation challenges and formulate specific recommendations. Further the recital suggests that the NIS CG could map national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the EU.

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.

I. General Remarks

In view of ensuring that NIS in central sectors of the economy are secure, Articles 14 and 16 NIS Directive introduce notification obligations as well as security requirements for OESs (Article 14) and DSPs (Article 16).

The different approaches in the transposition of the NIS Directive by Member States as well as pre-existing legislation challenges the determination of what needs to be reported. Additionally, the identification process of OES varies across Member States (see commentary to Article 5 NIS Directive), which in turn means that an entity may fall within the scope of the Directive in Member State A but not in Member State B due to different assessment criteria. As a consequence, an entity may have to report an incident in Member State A but not in Member State B. The same issues arise when determining whether an incident has to be reported because Member States may employ different approaches to measure the impact of incidents, i.e. different thresholds are set for surpassing the requirement of 'significant' impact.

II. In Detail

Article 14(1) Appropriate and Proportionate Technical and Organisational Security Measures

Article 14(1) NIS Directive requires the implementation of appropriate and proportionate technical and organizational measures to manage the risks posed to NIS security. To avoid imposing a disproportionate financial and administrative burden on OESs, the requirements should be proportionate to the risk presented by the NIS concerned, taking into account the state of the art of such measures. (cf. Recital 53 NIS Directive). The NIS Directive encourages the promotion and development of a culture of risk management, involving risk assessment

and the implementation of security measures appropriate to the risk involved (cf. Recital 44 NIS Directive).

Article 4(2) NIS Directive defines 'security of network and information systems' as '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'. This definition provides the four protection goals of NIS security: availability, authenticity, integrity and confidentiality.

The notion of 'appropriate' security measures highlights a major problem with the NIS Directive for legal and IT experts alike, namely, what can be considered 'appropriate' in this context. Again, the NISD only requires Member States to adopt measures to achieve a high common level of NIS security across the EU but leaves them a margin of discretion to achieve the objective, which will obviously lead to divergences. These divergences may in particular arise towards OES as the NIS Directive distinguishes between DSPs and OES, with stronger harmonisation in the field of DSPs (see commentary to Article 3 NIS Directive). It has to be noted, that during the legislative process for the NIS Directive it was agreed that DSPs should be subject to a 'light-touch' regime, meaning that DSPs should not be subject to the same strict obligations as OES given the greater risks that emanate from critical infrastructures.

In contrast to the section on DSP, which explicitly refers to 'compliance with international standards' (Article 16(1) NIS Directive) to be considered when assessing the level of security, Article 14 NIS Directive refrains from any such reference. For DSPs, technical guidelines published by ENISA (ENISA, 'Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers' (December 2016)) additionally define common baseline security objectives for DSPS. Furthermore, these guidelines also describe different levels of sophistication in the implementation of security objectives and map the objectives against well-known industry standards, national frameworks and certification schemes. Although Article 19(2) NIS Directive provides a legal basis for ENISA, in collaboration with Member States, to also draw up advice and guidelines for OES, this has not been pursued. However, the NIS CG provides an interactive table with minimum security measures for OES and has published guidance in the form of a reference document (NIS CG, 'Reference Document on security measures for Operators of Essential Services', CG Publication 01/2018) that summarizes the NIS CG's main findings on this subject matter.

As regards the practice of Member States, most national legislator seem to share the position that a principles-based approach is more effective than prescriptive rules when it comes to appropriate and proportionate security measures (see Mark D. Cole and Sandra Schmitz, 'The interplay between the NIS Directive and the GDPR in a cybersecurity threat landscape' [2019] University of Luxembourg FDEF Law Working Paper Series, Paper no. 2019-017, p. 8). A

principles-based approach provides more flexibility in a complex and rapidly changing IT environment.

Where national implementations or guidance or EU legislation in context of IT security contain reference to 'state of the art' technology, legislators, however, usually refrain from defining what state of the art in IT security exactly means. Accordingly, also Article 14(1) NIS Directive does not explain how state of the art technology has to be construed. Commonly, the notion refers to the highest level of general development achieved at a particular time. In law, the notion has some tradition in patent law (cf. for instance Article 54 Convention on the Grant of European Patents of 5 October 1973 (European Patent Convention) as well as in tort law (Cf. for instance Article 7(e) 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 (Product Liability Directive) [1985] OJ L 210/29). As regards the latter, it may be used as a legal defence, meaning that for instance a manufacturer cannot be held liable if he can prove that the state of technical and scientific knowledge, at the time when the product was put in circulation, was not such as to enable the existence of a certain defect to be discovered. In patent law, state of the art is used in the process of assessing and asserting the novelty of an invention. With increasing regulation of technology and in particular information technology, the notion of state of the art gained in importance. Similarly to the requirements on OESs and DSPs in the NIS Directive, Articles 25 and 32 GDPR require data controllers, and to some extent processors, to take the state of the art into account when implementing appropriate technical and organisational measures to mitigate the risks caused by their data processing activities. Furthermore, the EECC contains a similar provision in Article 40(1) EECC, that applies to public electronic communications networks or services regarding the security of their networks and services. None of these legal interventions provides a binding legal definition of the concept of state of the art in the context of IT security. For further deployment of the notion state of the art in the vast body of EU legislation, see Sandra Schmitz-Berndt, 'Conceptualising the legal notion of 'State of the Art' in the context of IT security', in: Micheal Friedewald et al. (eds.), *Privacy and Identity 2021*, IFIP AICT 644, https://doi.org/10.1007/978-3-030-99100-5_3, pp. 25-32.

The criterion of state of the art is a purely objective that does not take into account the individual means of the addressee. In the context of GDPR, state of the art has been defined by scholars as the procedures, equipment or operating methods available in the trade in goods and services for which the application thereof is most effective in achieving the respective legal protection objectives' (see Karsten Bartels and Merlin Backer, 'Die Berücksichtigung des Stands der Technik in der DSGVO' [2018] DuD 214). Accordingly, subjective elements such as high costs will justify a derivation from this. One may argue, that proprietary tools that are only offered by a single vendor to competitors under abusive conditions may not amount to methods that are available in a strict sense. However, the state of the art criterion always has to be placed in context. Legal interventions commonly require that the technical measure that respects the state of the art is inter alia 'appropriate'

(e.g. to the risks posed), 'proportionate to the cost of implementation', take into account the 'nature, scope, context and purpose of [data] processing' (GDPR) and/or risks. As regards the NIS Directive, Recital 53 specifies that in order to avoid imposing a disproportionate financial and administrative burden on OESs and DSPs, the requirements should be proportionate to the risk presented by the NIS concerned. This is in line with the state of the art requiring economically and technically feasible measures in corresponding legal interventions.

Furthermore, state of the art has to be distinguished from the state of science and technology, which relates to a very high level of protection, that requires to take into account the latest scientific knowledge regardless of whether it is technically feasible and available (see Sandra Schmitz-Berndt, 'Conceptualising the legal notion of 'State of the Art' in the context of IT security', in: Micheal Friedewald et al. (eds.), *Privacy and Identity 2021*, IFIP AICT 644, https://doi.org/10.1007/978-3-030-99100-5_3, p. 29).

Art. 14(2) Appropriate Measure to Prevent and Minimise the Impact of Incidents

Member States must ensure that OESs take appropriate measures not only to prevent but also to minimise the impact of incidents affecting NIS security with a view to ensuring the continuity of those services. Article 14(2) addresses the overall resilience of essential services aiming at the implementation of a continuity plan in case of interferences with the service provided.

Article 14(3) Notification of an Incident with Significant Impact

Article 14(3) NIS Directive requires Member States to ensure that OES notify, without undue delay, the competent authority or CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Article 16(3) NIS Directive introduces a similar obligation with regard to DSPs, which must notify any incident having a substantial impact on the provision of a service that they offer within the EU.

Member States are left with substantive freedom of choice as regards the implementation of the reporting obligation. First of all, Article 14(3) NIS Directive provides the Member States with an option as regards the receiving end of notifications: this may either be the competent authority or CSIRT. In the national implementation of the NIS Directive, Member States commonly determined either a CSIRT or authority in charge of receiving and handling incident notifications. However, the authority may also depend from sector to sector where Member States have implemented a decentralized supervisory regime (see commentary to Article 8 NIS Directive). Further, there is no harmonization of the reporting time window. Article 14(3) NIS Directive refers to the indefinite legal concept of 'without undue delay'. Section 11(3)(b(i) of the UK Network and Information Systems Regulations 2018 sets forth a time limit of 72 hrs, which matches the breach notification time limit in the GDPR, whereas the German transposition replicates the notion of 'undue delay' from the Directive.

Article 14(4) Determination of the Significance of an Impact

Article 4 (7) NIS Directive defines an incident as 'any event having an actual adverse effect on the security of network and information systems'. Since an adverse effect can easily be achieved, thus, the reporting obligation in terms of OES is limited to 'incidents having a significant impact on the continuity of the essential service they provide' (Article 14 (3) NIS Directive). In any case, some harm must have materialized since there must have been an effect on the continuity of the service. The NIS CG refers to ISO 22301 for a definition of business continuity that may be employed in this context, namely business continuity as the 'capability of the organization to continue delivery of products and services at acceptable predefined levels following disruptive incident' (See NIS CG, 'Reference document on incident notification for operators of essential services', p. 10).

As regards the significance of an impact, most Member States lack further guidance as to the determination of significance. Article 14(4) NIS Directive provides a list of parameters that shall be taken into account, namely '(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'. In that line Recital 27 of the NIS Directive specifies that the number of users affected by the disruption relate to the users relying on that service for private or professional purposes; their use of the service 'can be direct, indirect or by intermediation'. The amount of leeway as to the exact rules to be adopted may result in a variety of notification requirements which do not only vary from Member State to Member State but also within sectors.

Recital 47 NIS Directive foresees that competent authorities should retain the ability to adopt national guidelines concerning the circumstances of incident notifications by OES. Given the fundamental differences between OES and DSPs, in particular the direct link of OES with physical infrastructure, Member States are able to impose stricter requirements on OES than those laid down in the Directive (see Recital 57 NIS Directive).

Different approaches may be implemented in terms of parameters as well as regards thresholds. As regards parameters, Member States may determine that significance is only measured by the parameters enlisted in Article 14(4) NIS Directive; they may use an extended generic set of parameters or sector-specific parameters (see NIS CG, 'Reference document on incident notification for operators of essential services – circumstances of notification', CG Publication 02/2018, p. 15).

At EU level, guidelines published by the NIS CG (NIS CG, 'Guidelines on notification of operators of essential services incidents – formats and procedures', CG Publication 05/2018) as well as a the NIS CG Reference document (CG Publication 02/2018) provide some general guidance addressed at Member States on how incident notification provisions could effectively be implemented across the EU. As regards the 'significant impact' of an incident, the guidelines suggest taking into account the parameters listed in Article 6(1) NIS Directive, i.e. those

factors that are used to determine the significance of 'a disruptive effect'. Accordingly, when determining the significance of an impact on the service, Member States shall also consider

(a) the dependency of other OES sectors on the service provided by the affected entity;

(b) the impact that incidents have, in terms of degree and duration, on economic and societal activities or public safety;

(c) the market share of the entity concerned;

(d) 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.

The guidelines as well as the reference document provide some guidance as to how these factors should be interpreted at national level and address the challenges posed in some sectors in applying the parameters, however, they are neither binding nor specific enough for entities to rely on.

As regards thresholds, the NIS CG also identified three distinct approaches: generic thresholds for all sectors/subsectors, subsector based thresholds and a no thresholds policy, where all incidents have to be reported. The latter, however, renders the criterion of 'significance' at absurdum, when all incidents have to be reported.

Furthermore, mandatory reporting of all incidents or generic thresholds for all sectors contravene the ratio of the NIS Directive. As regards the factors enlisted in Article 6(1) NIS Directive, it must be noted that the impact assessment to be conducted for the determination of significant disruptive effect must inter alia consider sector-specific factors of which some are enlisted in Recital 28 of the NIS Directive; for instance, a sector-specific factor in the sector 'processing and supply of water production' would relate to the volume and number and types of users supplied, including for example, hospitals, public service organizations, or individuals, and the existence of alternative sources of water to cover the same geographical area. If the NIS CG considers the factors of Article 6(1) NIS Directive to be taken into account as parameters to measure the significance of an impact, then sectorial particularities have to be taken into account as well.

In consideration of the aforementioned, each Member State may decide to implement individual industry specific parameters and thresholds reflecting sector particularities and/or national particularities (NIS CG, 'Reference document on incident notification for operators of essential services – circumstances of notification', CG Publication 02/2018, p. 15). For instance, in Luxembourg, the Institut Luxembourgeouis de Régulation, which is the Luxembourgish regulatory authority for NIS entities with the exception of entities in the financial sector, determines the significance for each sector in a regulatory order following a public consultation (see for instance Règlement ILR/N23/1 du 2 mai 2023 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport sous-secteur transport aérien; Règlement ILR/N21/2 du 04

octobre 2021 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la Continuité des services essentiels du secteur eau potable). In contrast, in Denmark, every sector defines what constitutes a significant impact (European Commission et al., 'Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665', p. 51).

Fragmentation across EU Member States is not limited to diverging levels of guidance and diverging interpretations of 'significant', but also a direct result of various Member States having a reporting regime in place that goes much further than required by Article 14 NIS Directive. In these Member States reporting is not restricted to 'incidents having a significant impact on the continuity of the essential service they provide' (Article 14(3) NIS Directive), but also incidents that only have the potential to cause harm.

In Germany with its pre-existing legislation, § 8b IV BSIG (Act on the Federal Office for Information Security) requires operators of 'critical infrastructures' to report '1. incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems […] which have resulted in a failure or material impairment of the functionality of the critical infrastructures operated by them; as well as 2. significant incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems […] which may result in a failure or material impairment of the functionality of the critical infrastructures operated by them'. The explanatory memorandum to the IT Security Act 1.0, which introduced the aforementioned provision, outlines that an incident requires that there has been an interference of such a kind that the affected technology can no longer carry out its foreseen function or that the interference at least targeted the functioning (Deutscher Bundestag, BT-Drs. 18/4096 (25 February2015)). An incident can thus also be established where an attack has only been attempted or been successfully defended by security measures.

Similarly, the French implementation of the NIS Directive requires OES to report incidents that 'have or are likely to have, considering the number of users and the geographical area affected and the duration of the incident, a significant impact on the continuity of these services' (Article 7 Act No. 2018-133 of 26 February 2018 on various provisions for adapting to European Union law in the field of security (Loi no 2018-133 du 26 février 2018 portant diverses dispositions d'adaption au droit de l'Union européenne dans le domaine de la sécurité).

Accordingly, the 'significance' threshold varies from clear-cut sector-specific guidance regarding significant impact to incidents that have not materialized but have the potential to have a significant impact. The later exceeds the requirements of Article 14(3) NIS Directive, that there must have been a service disruption for a certain time across a certain area, that impacted economic and societal activities or public safety.

Article 14(5) Information of Affected Member States

If it can be established from the information provided by the OES that the incident also has a significant impact on the continuity of essential services in another Member States, the competent authority or the CSIRT shall inform the affected Member State. Any information that is transferred must preserve the security and commercial interests of the OESs as well as the confidentiality of the information provided in the notification.

Article 14(6) Disclosure to the Public

Publicity of incidents reported to the competent authorities or CSIRTs should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the OES reporting incidents (see Recital 59 NIS Directive). Accordingly, Recital 59 NIS Directive also requires competent authorities and the CSIRTs to pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

Disclosure of incidents also exist under Article 34, GDPR, where data controllers are required to notify the data subject without undue delay about a data breach in order to put the data subject in a position to take necessary precautions to prevent potential harm from materialising or limit the effects of the data breach. In contrast to the GDPR, there is no such obligation for the OES. Instead it is up to the competent authority or the CSIRT to determine whether public disclosure is necessary. Since a security incident in the sense of the NIS Directive may also involve personal data, cooperation and coordination will be necessary between the competent authorities under the NIS Directive and DPAs to not hamper NIS security by early disclosure (see Sandra Schmitz-Berndt and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' [2021] IRLCT 101'; 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' [2021] JIPITEC 447, 451 et seq.).

It has to be noted that the notification regimes under the NIS Directive and the GDPR coexist: they are neither mere duplications, nor do they exclude one another in consideration of their distinct protection goals (information security/privacy).

Article 14(7) Guidelines for Incident Notification

A NIS CG 'Reference document on incident notification for operators of essential services – circumstances of notification' (CG Publication 02/2018), as well as guidelines published by the NIS CG (NIS CG, 'Guidelines on notification of operators of essential services incidents – formats and procedures', CG Publication 05/2018) provide some general guidance addressed at Member States on how incident notification provisions could effectively be implemented across the EU.

III. Review of the NIS Directive

Within the public consultation in course of the NIS Directive review process, a general agreement among stakeholders could be observed in terms of reporting thresholds for both,

OESs and DSPs, being set too high to trigger the notification obligation. According to the review study report (European Commission et al., 'Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665, Final Study Report'), a significant number of national competent authorities 'called for harmonizing reporting thresholds' for incidents since 'hardly any incident in the past two years has attained one of the established thresholds'. In fact, the number of reports received by different national authorities varied significantly (see Sandra Schmitz-Berndt, 'Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive' [2023] Journal of Cybersecurity, https://doi.org/10.1093/cybsec/tyad009).

IV. Outlook: NIS 2 Directive

Article 23 NIS 2 Directive provides a uniform reporting regime for important and essential entities. Article 23(1) NIS 2 Directive requires the notification of incidents that are significant, with Article 23(3) NIS 2 Directive defining when an incident shall be considered to be significant. An incident is considered significant, when '(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage'. Accordingly, the threshold has been lowered significantly when also incident have to be reported that are 'capable' of causing severe harm. Further, an obligation to notify the service recipient of measures or remedies that they should take in response of a significant cyber threat has been adopted (Article 23(2) NIS 2 Directive). The extension of the reporting obligation has received a lot of controversy during the negotiations (see Sandra Schmitz-Berndt, 'Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive' [2023] Journal of Cybersecurity, https://doi.org/10.1093/cybsec/tyad009).

Besides the scope of reporting, the NISD 2 Directive also addresses the format and procedure. Notably, Article 23(4) NIS 2 Directive introduces a tiered reporting procedure consisting of an early warning, a formal incident notification and a final report. Article 23(4)(a) NIS 2 Directive specifies that the first 'early warning' has to be submitted 'without undue delay and in any event within 24 hours of becoming aware of the significant incident'. This early warning only has to contain some basic information in relation to the incident and a potential cross-border impact. Other than the previous regime, the reporting procedure also foresees initial feedback by the CSIRT or competent authority; such feedback is already mandatory to the early warning (Article 23(5) NIS 2 Directive). Furthermore, the entity concerned is entitled to request guidance or operational advice on the implementation of possible mitigation measures. In the following, the actual incident notification has to be submitted to the CSIRT or competent authority within 72 hours of becoming aware of the significant incident. This notification should update the information contained in the early warning and indicate an initial assessment of the significant incident, including its severity

and impact, as well as, where available, the indicators of compromise (Article 23(4)(b) NIS 2 Directive). The CSIRT or competent authority is further entitled to request an intermediate report on relevant status updates (Article 23(4)(c) NIS 2 Directive). A final report has to be handed in not later than one month after the submission of the actual incident notification (Article 23(4)(d) NIS 2 Directive). This final report must include the following: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; and (iv) where applicable, the cross-border impact of the incident. If the incident is still ongoing at the time of the final report, the final report should be replaced by a progress report and a final report within one month after the incident has been handled.

Although not in the operative part but only in the Recitals, the legislator expresses its dissatisfaction with the fragmentation of incident reporting. In that regard, Recital 94, proposes the use of a single entry point for the reporting of NIS incidents under the NIS 2 Directive and corresponding sectoral regimes to achieve a common and automatic incident reporting. Furthermore, Recital 30 requests Member States to streamline supervisory activities between the competent authorities under the NIS 2 Directive and the CER Directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L333/164) which shall also include an endeavour to harmonise incident notification templates.

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.

I. General Remarks

In view of ensuring that NIS in central sectors of the economy are secure, Articles 14 and 16 NIS Directive introduce notification obligations as well as security requirements for OESs (Article 14) and DSPs (Article 16).

In contrast to Article 14 (3) NIS Directive, which applies solely to OES, the reporting obligation for DSPs in Article 16 (3) NIS Directive relates to incidents that have 'a substantial impact' on the provision of a service 'that they offer within the Union'.

II. In Detail

Article 16(1) Appropriate and Proportionate Technical and Organisational Security Measures

Article 16(1) NIS Directive requires the implementation of appropriate and proportionate technical and organizational measures to manage the risks posed to NIS security. As foreseen in Article 14(1) NIS Directive in relation to OESs, the requirements should be proportionate to the risk presented by the NIS concerned, taking into account the state of the art of such measures. (cf. Recital 53 NIS Directive). The NIS Directive encourages the promotion and development of a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risk involved (cf. Recital 44 NIS Directive).

With stronger harmonisation as regards DSPs, Article 16(1) NIS Directive specifically mentions 'compliance with international standards' to be considered when assessing the level of security. In accordance with Article 19(2) NIS Directive, ENISA published technical guidelines for the implementation of minimum security measures for DSPs under the NIS Directive (ENISA, 'Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers' (December 2016)) based on its previous Cloud Certification Schemes Meta framework (CCSM) (which has been further advanced under the heading EUCS (ENISA, 'EUCS – Cloud Services Scheme' (December 2020)). These guidelines aim to define common baseline security objectives for DSPs, describe different levels of sophistication in the implementation of security objectives and to map the security objectives against well-known industry standards, national frameworks and certifications schemes (such as ISO/IEC 27001:2013; CSA CCM (Clouds Control Matrix v3.0.1); BSI C5 (Cloud Computing Compliance Controls Catalogue as of February 2016); COBIT5 (Framework for the governance and management of enterprise IT); CCS CSC (CIS Critical Security Controls for Effective Cyber Defence, version 6.1. as of 31 August 2016); OCF (CSA Star Program & Open Certification Framework in 2016 and beyond); NIST, Framework for Improving Critical Infrastructure Cybersecurity (version 1.0 as of 12 February 2014); PCI DSS (Payment Card Industry Security Standards Councils, Data Security Standard Requirements and Security Assessment Procedures (version 3.2. as of April 2016); CES (Cyber Essentials Scheme, June 2014). The overall objective is the

establishment of a common approach regarding security measures for DSPs in order to avoid fragmentation through nationally divergent standard compliance requirements.

In accordance with Article 16(8) NIS Directive the European Commission issued a Commission Implementing Regulation in that regard, which inter alia lays down further specification of the elements to be taken into account by DSPs for managing the risks posed to the security of network and information systems (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, [2018] OJ L26/48). However, the Regulation does not specifically mention industry standards such as ISO/IEC 27001:201332 or the NIST Cybersecurity Framework, and thus frameworks DSPs may certify against and use the certification to demonstrate compliance. Even the legislator recognized in Recital 66 that it 'might be helpful to draft harmonised standards'. Pursuant to the Implementing Regulation, the security of network and information systems and their physical environment shall include the following elements:

(a) the systematic management of network and information systems, which means which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, incl. risk analysis, human resources, security of operations, security architecture, secure data and system lifecycle 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 authorized and restricted based on business and security requirements.

No further guidance is provided in the Implementing Regulation.

Art. 16(2) Appropriate Measure to Prevent and Minimise the Impact of Incidents

Member States must ensure that DSPs take appropriate measures not only to prevent but also to minimise the impact of incidents affecting NIS security with a view to ensuring the

continuity of those services. Article 16(2) addresses the overall resilience of digital services aiming at the implementation of a continuity plan in case of interferences with the service provided.

Article 16(3) Notification of an Incident with Substantial Impact

Article 16(3) NIS Directive requires Member States to ensure that DSPs notify, without undue delay, the competent authority or CSIRT of incidents having a substantial impact on the provision of a service that they offer within the EU. Article 14(3) NIS Directive introduces a similar obligation with regard to OESs, which must notify any incident having a significant impact on the continuity of the essential services they provide.

Article 16(4) Determination of a Substantial Impact

In order to determine whether the impact of an incident is substantial, Article 16(4) NIS Directive enlists parameters to be taken into account. One year ahead of the transposition deadline of the NIS Directive, ENISA specified the parameters used to measure the impact of an incident in a guideline (ENISA. 'Incident Notification for DSPs in the Context of the NIS Directive' (27 February 2017). In consideration of the difficulties of determining the 'substantial impact', the Commission further adopted the 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 ([2018] OJ L26/48). Article 4 of the Commission Implementing Regulation sets forth that an incident has 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.

Recital 10 of the Regulation clarifies that the cases laid down in this Regulation 'should be considered as a non-exhaustive list of substantial incidents'. Comprehensive guidelines on quantitative thresholds of notification parameters could however be set up in the future based on the lessons learnt from the application of the Regulation and best practice

information collected by the NIS Cooperation Group (Recital 10 Commission Implementing Regulation (EU) 2018/151). It has to be noted that Implementing Regulations are directly applicable and need not be transposed into national legislation which ensures a coherent application across Member States.

Article 16(5) Notification of an Incident by an OES

Where an OES relies on a third-party DSP for the provision of an essential service, any significant impact on the essential service's continuity due to an incident affecting the DSP shall be notified by the OES affected.

Article 16(6) Information of Affected Member States

If it can be established from the information provided by the DSP that it is appropriate, the competent authority or the CSIRT shall inform other affected Member States. This is in particular the case where the incident concerns two or more Member States. Any information that is transferred must preserve the security and commercial interests of the DSP as well as the confidentiality of the information provided in the notification.

Article 16(7) Disclosure to the Public

Publicity of incidents reported to the competent authorities or CSIRTs should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the DSP reporting incidents (see Recital 59). Accordingly, Recital 59 also requires competent authorities and the CSIRTs to pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

Article 16(8) Implementing Acts on Article 16(1) and 16(4)

In accordance with Article 16(8) NIS Directive the European Commission issued a Commission Implementing Regulation in that regard, which inter alia lays down further specification of the elements to be taken into account by DSPs for managing the risks posed to the security of network and information systems (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, [2018] OJ L26/48).

Article 16(9) Implementing Acts on Notification Requirements

The Commission did not adopt an implementing act laying down the formats and procedures applicable to notification requirements. A comprehensive guideline on how to implement incident notification for DSPS in the context of the NIS Directive has however been published by ENISA in February 2017 (ENISA. 'Incident Notification for DSPs in the Context of the NIS Directive' (27 February 2017)). These guidelines assess incident notification as part of the overall

incident management process and provide examples for the types of incidents covered by the NIS Directive.

Article 16(10) Prohibition on Further Security or Notification Requirements

In consideration of the harmonisation approach towards DSPs, Member States shall not impose any further security or notification requirements on DSPs.

Article 16(11) No Application to SMEs

Chapter V of the NIS Directive shall not apply to SMEs as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium–sized enterprises ([2003] OJ L124/36).

III. Review of the NIS Directive

Within the public consultation in course of the NIS Directive review process, a general agreement among stakeholders could be observed in terms of reporting thresholds for both, OESs and DSPs, being set too high to trigger the notification obligation. According to the review study report (European Commission et al., 'Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665, Final Study Report'), a significant number of national competent authorities 'called for harmonizing reporting thresholds' for incidents since 'hardly any incident in the past two years has attained one of the established thresholds'. In fact, the number of reports received by different national authorities varied significantly (see Sandra Schmitz-Berndt, 'Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive' [2023] Journal of Cybersecurity, https://doi.org/10.1093/cybsec/tyad009).

IV. Outlook: NIS 2 Directive

Article 23 NIS 2 Directive provides a uniform reporting regime for important and essential entities. Article 23(1) NIS 2 Directive requires the notification of incidents that are significant, with Article 23(3) NIS 2 Directive defining when an incident shall be considered to be significant. An incident is considered significant, when '(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage'. Accordingly, the threshold has been lowered significantly when also incident have to be reported that are 'capable' of causing severe harm. Further, an obligation to notify the service recipient of measures or remedies that they should take in response of a significant cyber threat has been adopted (Article 23(2) NIS 2 Directive). The extension of the reporting obligation has received a lot of controversy during the negotiations (see Sandra Schmitz-Berndt, 'Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive' [2023] Journal of Cybersecurity, https://doi.org/10.1093/cybsec/tyad009).

Besides the scope of reporting, the NISD 2 Directive also addresses the format and procedure. Notably, Article 23(4) NIS 2 Directive introduces a tiered reporting procedure consisting of an early warning, a formal incident notification and a final report. Article 23(4)(a) NIS 2 Directive specifies that the first 'early warning' has to be submitted 'without undue delay and in any event within 24 hours of becoming aware of the significant incident'. This early warning only has to contain some basic information in relation to the incident and a potential cross-border impact. Other than the previous regime, the reporting procedure also foresees initial feedback by the CSIRT or competent authority; such feedback is already mandatory to the early warning (Article 23(5) NIS 2 Directive). Furthermore, the entity concerned is entitled to request guidance or operational advice on the implementation of possible mitigation measures. In the following, the actual incident notification has to be submitted to the CSIRT or competent authority within 72 hours of becoming aware of the significant incident. This notification should update the information contained in the early warning and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise (Article 23(4)(b) NIS 2 Directive). The CSIRT or competent authority is further entitled to request an intermediate report on relevant status updates (Article 23(4)(c) NIS 2 Directive). A final report has to be handed in not later than one month after the submission of the actual incident notification (Article 23(4)(d) NIS 2 Directive). This final report must include the following: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; and (iv) where applicable, the cross-border impact of the incident. If the incident is still ongoing at the time of the final report, the final report should be replaced by a progress report and a final report within one month after the incident has been handled.

Although not in the operative part but only in the Recitals, the legislator expresses its dissatisfaction with the fragmentation of incident reporting. In that regard, Recital 94 NIS 2 Directive, proposes the use of a single entry point for the reporting of NIS incidents under the NIS 2 Directive and corresponding sectoral regimes to achieve a common and automatic incident reporting. Furthermore, Recital 30 NIS 2 Directive requests Member States to streamline supervisory activities between the competent authorities under the NIS 2 Directive and the CER Directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L333/164) which shall also include an endeavour to harmonise incident notification templates.

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.

I. General Remarks

Article 18 NIS Directive outlines the jurisdictional rules applicable to DSPs. Jurisdictional rules define the territorial links or connecting factors that will be considered relevant to establish jurisdiction in cases with cross-border elements.

II. In Detail

The NIS Directive subjects OESs and DSPs to different jurisdictional regimes: it uses concurrent jurisdictional rules for cross-border OESs and exclusive jurisdictional rules for DSPs. This means that, while cross-border OESs are subject to the jurisdiction of each of the Member States where they provide their services in parallel, DSPs are subject only to the jurisdiction of the Member State where they have their main establishment.

Preliminary Remark: Jurisdictional Rules Applicable to OESs

The jurisdictional rules applicable to OESs must be inferred from Article 5 and Recitals 21 and 24 NIS Directive.

According to Article 5 NIS Directive, Member States must identify the OESs that have an establishment within their territory, and if an entity provides an essential service in two or more Member States, before the decision on the identification is taken, those Member States must engage in consultation with each other. Recital 24 clarifies that the consultation process is intended to help them to assess the critical nature of the operator in terms of cross-border impact, allowing each Member State involved to present its views regarding the risks associated with the services provided (NIS Cooperation Group, 'NIS Cooperation Group,

Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact', CG Publication 07/2018). In addition, Recital 21 provides that for the purposes of identifying OESs, establishment implies the effective and real exercise of activity through stable arrangements, irrespective of the legal form of such arrangements.

In view of the foregoing, it follows that companies identified as OESs will be subject to the jurisdiction of the Member State where they provide essential services. Additionally, if those companies provide essential services in more than one Member State, they will be subject to the jurisdiction of each of those Member States in parallel. Thus, several Member States can concurrently have jurisdiction over the same OES if, for example, it has branch offices —or anything that amounts to an establishment under domestic law— in different Member States (see commentary to Article 5 NIS Directive). Moreover, as the Directive follows a minimum harmonisation approach regarding OES, Member States are free to impose requirements on OES that are higher than those provided for in the Directive (see commentary on Article 3 NIS Directive). Consequently, companies identified as OES in more than one Member State will need to comply with security and reporting requirements that vary greatly across Member States.

Jurisdictional Rules Applicable to DSPs

The jurisdictional rules applicable to DSPs are set out in Article 18 and Recitals 64 and 65 NIS Directive.

Unlike OESs, DSPs are only subject to the jurisdiction of a single regulator across the EU (one-stop-shop approach) based on where they have their main establishment which in principle corresponds to their head office. Recital 64 clarifies that the physical location of the network and information systems is not the determining factor of the main establishment. In addition, DSPs that are not established in the EU but that offer services in the EU, need to designate a representative established in one of the EU countries where they offer services, and they will be subject to the jurisdiction of the Member State where the representative is established. Moreover, according to the clarifications provided by the EU Commission, if DSPs not established in the EU fail to designate a representative, all the Member States where they offer services can in principle take action against them if they infringe their obligations deriving from the NIS Directive (European Commission, 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, Annex 1).

III. Review of the NIS Directive

During the review process, numerous problems with the jurisdictional rules of the NIS Directive were identified.

In this sense, for example, it was pointed out that under the current rules cross-border OESs must deal concurrently with a multiplicity of NIS national competent authorities in each of the different Member States where they are identified as OES, and additionally, they need to sort out an uneven landscape regarding applicable security and reporting obligations. Moreover, the national approaches for identifying OES are not consistent. All this creates a multilevel fragmentation of the internal market that can make compliance extremely burdensome and can potentially give rise to divergent implementations of the Directive across the EU.

Regarding DSPs, it was noted that the one-stop-shop mechanism introduced by the NIS Directive carries with it a risk of "regulatory shopping" given that DSPs could structure their operations to place their main establishment in the Member State where they believe they would receive a more favourable treatment from the regulator or where they would face more lenient penalties. Furthermore, it was pointed out that the one-stop-shop mechanism could lead to centralizing oversight around regulators that may not have the adequate technical, financial, and human resources to carry out the tasks assigned to them, creating delays and inertia.

IV. Outlook: NIS 2 Directive

The NIS 2 Directive abandons the distinction between OESs and DSPs and, in turn, introduces the aforementioned distinction between 'essential' and 'important' entities.

Article 24 and Recital 63 of the NIS 2 Proposal originally provided that, as a rule, all essential and important entities will fall under the jurisdiction of the Member State where they provide their services. And, if the entity provides services in more than one Member State, it would fall under the separate and concurrent jurisdiction of each of these Member States. However, this general rule underwent several amendments during the trilogue negotiations. Jurisdiction of the Member State where the service is provided only remains in relation to providers of public electronic communications networks or providers of publicly available electronic communications services (Article 26(1)(a) NIS 2 Directive) .

The general rule on jurisdiction is enshrined in Article 26(1) NIS 2 Directive, whereby entities falling within the scope of the NIS 2 Directive fall under the jurisdiction of the Member State in which they are established.

Besides the exception provided for providers of public electronic communications networks or providers of publicly available electronic communications services, Article 26(1)(b) and (c) NIS 2 Directive enlist further exceptions.

DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms should be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union (Article 26(1)(b) NIS 2 Directive). This jurisdictional rule takes account of the cross-border nature of the services and operations of these type of providers, stipulating that only one Member State should have jurisdiction over those entities (cf. Recital 114 NIS 2 Directive). Jurisdiction is attributed to the Member State in which the entity concerned has its main establishment in the EU. Recital 114 NIS 2 Directive elaborates on the criterion of establishment for the purposes of the NIS 2 Directive and sets forth that this implies the effective exercise of activity through stable arrangements. Further, Recital 114 NIS 2 Directive clarifies that the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Moreover, the main establishment should be considered to be in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken in the European Union, which will typically correspond to the place of the entities' central administration in the Union (Recital 114 NIS 2 Directive). If such a Member State cannot be determined or if such decisions are not taken in the European Union, Recital 114 NIS 2 Directive provides alternative criteria, which should be applicable in descending order until a determination is possible: the main establishment should be considered to be in the Member State where cybersecurity operations are carried out; if not applicable, the main establishment should be considered to be where the entity has the establishment with the highest number of employees in the Union.

An exception is provided for publicly available recursive DNS service which provided by a provider of public electronic communications networks or of publicly available electronic communications services only as a part of the internet access service; in this case, jurisdiction is attributed to all the Member States where the services are provided (Recital 115 NIS 2 Directive).

While public administration entities, in general, fall under the jurisdiction of the Member State which established them, an alternative rule shall apply if the entity provides services or is established in more than one Member State; the entity shall fall under the separate and concurrent jurisdiction of each of those Member States, which will be required to cooperate and provide mutual assistance (cf. Recital 115 NIS 2 Directive).

Recital 116 NIS 2 Directive emphasizes that where a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider or a provider of an online marketplace, of an online search engine or of a social networking services platform, offers

services but is not established in the Union, it should designate a representative in the Union. For the requirement 'offering services', the mere accessibility in the Union of the entity's or an intermediary's website or of an email address or other contact details, or the use of a language generally used in the third country where the entity is established, should be considered to be insufficient (Recital 116 NIS 2 Directive). 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 language, or the mentioning of customers or users who are in the Union, could make it apparent that the entity is planning to offer services within the Union (ibid).

Chapter VI Standardisation and Voluntary Notification

Not part of this excerpt

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.

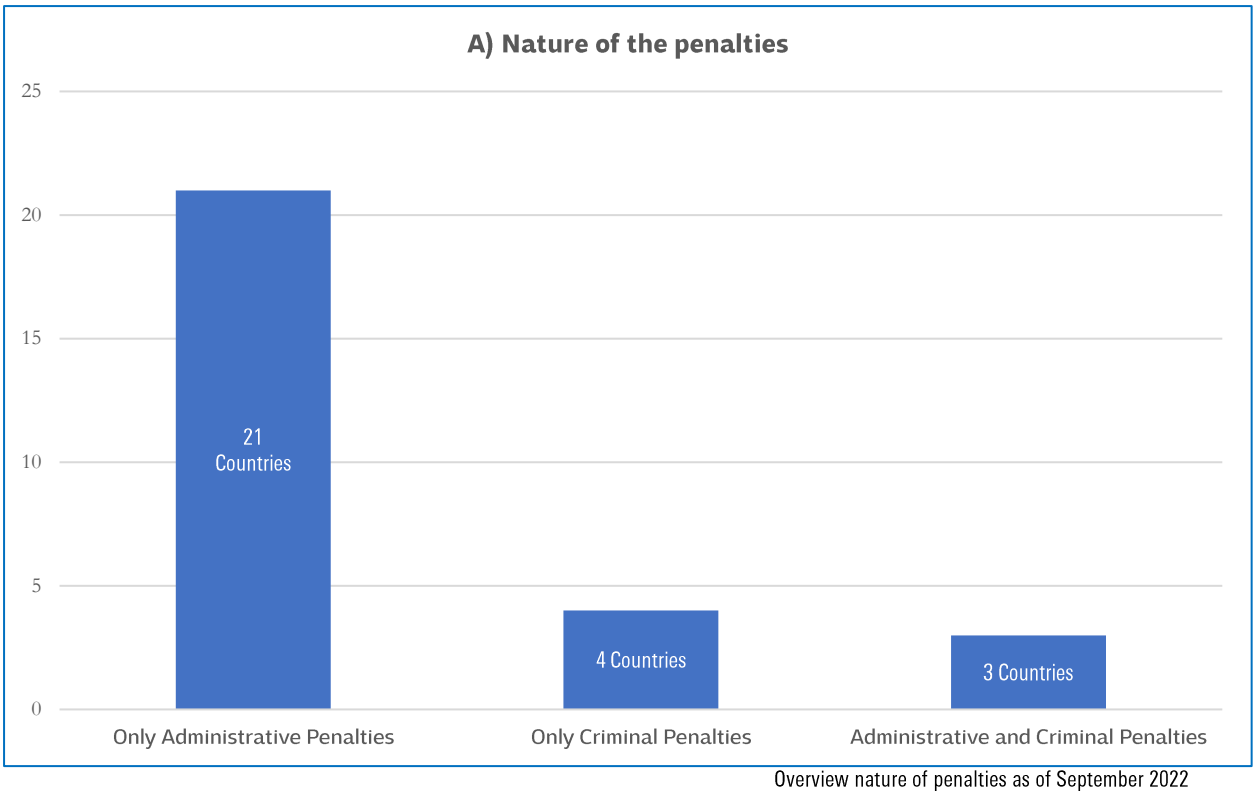
I. General Remarks

Article 21 NIS Directive provides that Member States must lay down the rules on penalties applicable to infringements of the national transposition measures. The penalties are set and enforced at national level according to the specificities of each Member State's legal system. The choice of penalties remains within the Member States' discretion. Accordingly, Member States can choose the measures which they consider most appropriate in terms of nature and severity as long as the penalties provided for under national law are effective, proportionate, and dissuasive. Finally, Article 21 stipulates that Member States must notify the Commission, without delay, of any amendment concerning the rules on penalties.

II. In Detail

Nature of Penalties Regime

There is great variation across Member States as regards the nature of the penalties' regime. When transposing Article 21 NIS Directive , the majority of Member States (21 Member States) opted for an administrative penalties' regime. Four Member States rely on criminal penalties (Croatia, Ireland, Estonia, and Slovenia); and finally, three Member States implemented a dual system that includes both, administrative and criminal penalties (Belgium, Cyprus, and Slovakia).



Overview nature of penalties as of September 2022

Severity of Penalties

According to the principle of sincere cooperation enshrined in Article 4(3) TFEU, Member States are under a general obligation to ensure that EU law is applied and enforced effectively (cf. C-40/04 *Yonemoto*, ECLI:EU:C:2005:519, para. 59).

An effective penalty is considered as one that ensures that the same diligence and strictness is applied for infringements of EU law and infringements of national law of similar nature and importance (cf. C-382/09 *Stils Met*, ECLI:EU:C:2010:596, para. 44; C-68/88 *Commission v Greece*, ECLI:EU:C1989:339, paras. 24 et seq.).

The criteria of effectiveness, proportionality and dissuasiveness are commonly used in secondary EU law without obliging Member States to adopt specific sanctions.

The severity of the sanctions must be commensurate to the seriousness of the breaches for which they are imposed, in particular by ensuring a genuinely dissuasive effect (C-81/12 *Asociaţia Accept*, ECLI:EU:C:2013:275, para. 63, with reference to Case C-383/92 *Commission* v *United Kingdom*, ECLI:EU:C:1994:234, para. 42, and C-180/95 *Draehmpaehl*, ECLI:EU:C:1997:208, para. 40) while respecting the general principle of proportionality (see, to that effect, C-101/01 *Lindqvist*, ECLI:EU:C:2003:596,paras. 87 et seq., and C-430/05 *Ntionik and Pikoulas*, ECLI:EU:C:2007:410, para. 53).

A penalty is proportionate when it is appropriate to attain the objectives set by the legislation in question and does not go beyond what is necessary in order to attain these objectives (cf. C-129/16 *Túrkevei Tejtermelő Kft.*, ECLI:EU:C:2017:547, para. 66 with further

references). In sum, the answer to the question of whether a penalty in a specific situation is effective, proportionate and dissuasive depends on the merits of the case. However, the thresholds set at national law must as such provide for the imposition of a penalty that fulfills the criteria set by the NIS Directive.

A comparative analysis of the national transposition measures has shown that there is great variation in the severity of the fines that Member States can potentially apply for violations of their national transposition measures. Most Member States have included caps in the range of EUR 100,000-1,000,000. The upper outlier is the United Kingdom with fines up to approx. EUR 20,000,000 (Section 18(6) Network and Information Systems Regulations 2018), which corresponds to the maximum administrative fine under Article 83(5) and (6) GDPR. The lower outlier is Lithuania with the maximum fine applicable set at approx. EUR 6,000. Some Member States also differentiate between the addressees of a penalty; for instance, in France, administrative fines differ for OESs (maximum fine: EUR 125,000) and DSPs (maximum fine: EUR 100,000). Additionally, in some Members States there is no minimum penalty but only a maximum penalty, giving full flexibility to the national authority.

It is also worth highlighting that Belgium and Cyprus provide prison terms as penalties for violations of their national transposition measures. Pursuant to Article 51 of the Belgian Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (Law establishing a framework for the security of network and information systems of general interest for public security), any natural person failing to comply with inter alia the incident reporting or security obligations shall be punished by imprisonment for a term of eight days to one year.

The table on the following pages provides an overview of the variety of penalties under the national transposition measures of the NIS Directive.

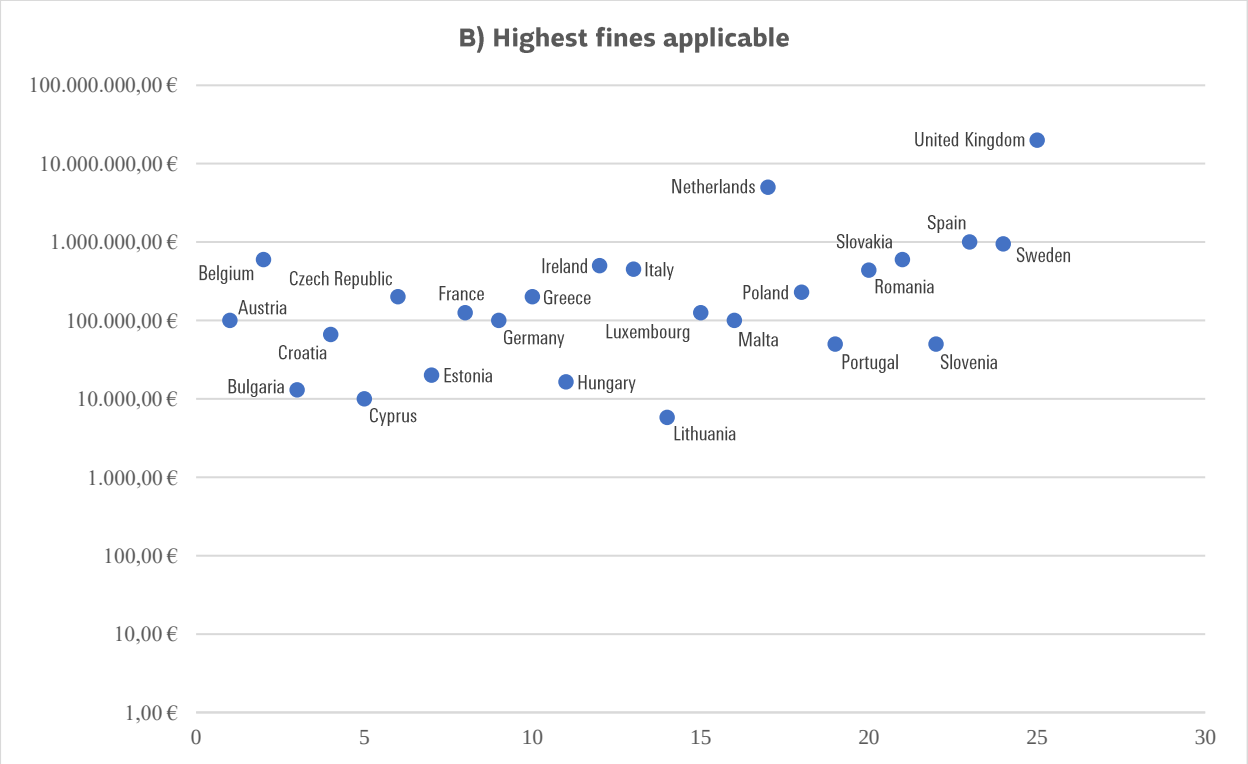
Country	Applicable legal provisions	Penalties
AUSTRIA	Section 26 of the Network and Information System Security Act.	Administrative penalties: • Fines up to EUR 50,000. • Fines up to EUR 100,000 in case of recurrence. • Fines may apply to individuals and legal entities. However, punishment of an individual pursuant to § 9 Administrative Penal Act 1991 (VStG), Federal Law Gazette No. 52/1991, may be waived if an administrative penalty is already being issued against the legal entity for the same offence. • ***Double jeopardy:*** fines do not apply if the act constitutes an offence falling within the jurisdiction of the ordinary courts or is punishable by a more severe penalty under other administrative penal provisions.
BELGIUM	Articles 51 and 52 of the Act of 7 of April 2019 Establishing a Framework for the Security of Network and Information Systems of General Interest for Public Security.	Criminal penalties: • Imprisonment from 8 days up to 2 years, and from 15 days up to 3 years in case of repeated offences. • Fines from EUR 26 up to 75,000. (Multiplication factor 8 ×: EUR 208 up to 600,000). They can be doubled in case of repeated offences. Administrative penalties: • Fines from EUR 500 up to 200,000. They can be doubled in case of repeated offences. • ***Double jeopardy:*** administrative fines can be applied only if the Prosecutor decides not to institute criminal proceedings.
BULGARIA	Articles 28, 29 and 30 of the Cybersecurity Act.	Administrative penalties: • Fines from BGN 1,000 up to 15,000 (approx. from EUR 500 up to 7,600) for violations of incident reporting obligations. In case of repeated violations, the fines range from BGN 2,000 up to 20,000 (approx. from EUR 1,000 up to 10,200). • Fines from BGN 1,000 up to 15,000 (approx. from EUR 500 up to 7,600) for failure to provide certain information and evidence or failure to comply with mandatory instructions. In case of repeated violations, the fines range from BGN 2,000 up to 25,000 (approx. from EUR 1,000 up to 13,000). • Fines from BGN 1,000 up to 15,000 (approx. from EUR 500 up to 7,600) for other violations.
CROATIA	Articles 42, 43, 44 and 45 of the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers.	Criminal penalties (minor offences): • Fines from HRK 15,000 up to 500,000 (approx. EUR 2,000 up to 66,400) to OESs and DSPs that fail to comply with the Act. • Fines from HRK 5,000 up to 150,000 (approx. from EUR 670 up to 20,000) to the individual craftsman or other self-employed individual that fails to comply with the Act. • Fines from HRK 2,000 up to 50,000 (approx. from EUR 265 up to 6,700) to the responsible person in the legal entity and the responsible person in the public entity that fails to comply with the Act.
CYPRUS	Sections 15, 16 and 30 of the Security and Information Systems Act of 2018.	Criminal Penalties: • Imprisonment up to 6 months and/or fine of up to EUR 10,000 to any person who prevents any employee of the competent authority to fulfil his duties. • Imprisonment up to 6 months and/or fine of up to EUR 10,000 to any person who breaches the Network and Information Security Law, the regulations or the decisions of the competent authority. Administrative Penalties: Fines up to EUR 8,500 for violations of the Network and Information Security Law or the decisions of the competent authority.
CZECH REPUBLIC	Section 15 of the Act No 205/2017 amending Act No 181/2014 on cybersecurity and amending related acts (the Cybersecurity Act), as amended by Act No 104/2017 and certain other acts.	Administrative Penalties: Fines up to EUR 200,000.
DENMARK	Act No. 436 of 8 May 2018.	Administrative Penalties: Denmark has not included a range for fines in the NIS Act. On license-based sectors, non-compliance with the NIS Act could result in the loss of the license.
ESTONIA	Section 18 of the Cybersecurity Act.	Criminal Penalties (minor offences): Fines up to EUR 20,000.
FINLAND	The NIS Directive was implemented by modifying 12 existing sector specific acts: the Act on Electronic Communications Services, the Aviation Act, the Railway Act, the Vessel Traffic Service Act, the	No new sanctions have been included as result of the transposition of the NIS Directive therefore the existing sector specific sanctions remain applicable.

Country	Applicable legal provisions	Penalties
	Act on the Safety and the Supervision of Security Operations of Certain Vessels and Ports Servicing them, the Act on Transport Services, the Electricity Market Act, the Natural Gas Market Act, the Act on the Supervision of Electricity and Gas Markets, the Water Services Act, the Act on the Financial Supervision and the Act on the National Supervisory Authority for Welfare and Health.	
France	Articles 9 and 15 of the Act No. 2018-133 of 26 February 2018 on various provisions for implementing European Union law in the field of security.	Administrative Penalties: • Fines up to EUR 125,000 to Operators of Critical Services. • Fines up to EUR 100,000 to DSPs.
Germany	Section 14 of the Act on the Federal Office for Information Security.	Administrative Penalties: Fines up to EUR 100,000.
Greece	Articles 13, 14 and 15 of the Ministerial Decision on the implementation measures of the Law No. 1027/4 October 2019.	Administrative Penalties: • Fines from EUR 15,000 up to 200,000 in the event of no notification or delay of notification. • Fines from EUR 50,000 up to 200,000 in the event of failure to take appropriate organizational or technical measures to manage the risks to network and system security. • Fines from EUR 50,000 to 200,000 in case of non-provision or unjustified delay in the provision of information, if requested by the National Cybersecurity Authority.
Hungary	Annex 1 of the Government Decree 187/2015 (VII.13) and Sec. 9 (2) of Government Decree 65/2013 (III.8).	Administrative Penalties: • Fines from HUF 50,000 up to 5,000,000 (approx. from EUR 165 up to 16,500) to DSPs. • Fines from HUF 100,000 up to 3,000,000 (approx. from EUR 330 up to 9,900) to OESs.
Ireland	Section 34 of the Statutory Instrument No. 360 of 2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems).	Criminal Penalties: • In case of summary conviction, fines from EUR 4,000 up to 5,000. • In case of conviction or indictment, fines up to EUR 50,000 to individuals and up to 500,000 to legal entities.
Italy	Article 21 of the Legislative Decree No. 65 of 18 May 2018.	Administrative Penalties: • Fines from EUR 4,000 up to 120,000 to DSPs. • Fines from EUR 12,000 up to 150,000 to OESs. • In case of repeated violations the applicable sanctions can be tripled.
Latvia	Law on Information Technology Security	Administrative Penalties: The Supervisory Committee of Digital Security can enforce its decisions in accordance with Administrative Procedure Law: it can issue warnings and impose pecuniary penalties.
Lithuania	Article 154 (11) and (12) of the Code of Administrative Offences	Administrative Penalties: • Warning • Fines up to EUR 5,792
Luxembourg	Article 14 of the Act of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of network and information system security in the European Union and amending 1° the amended Act of 20 April 2009 establishing the State Information Technology Centre and 2° the Act of 23 July 2016 establishing a High Commission for National Protection.	Administrative Penalties: • Warning • Reprimand • Fines up to EUR 125,000.
Malta	Article 19 of the European Union Act (CAP.460), Measures For High Common Level of Security of Network and Information Systems Order, 2018.	Administrative Penalties: • Warning • Cessation order • Fines from EUR 500 up to 100,000.
Netherlands	Article 29 of the Act of 17 October 2018 laying down rules for the implementation of Directive (EU) 2016/1148 (Network and Information Systems Security Act).	Administrative Penalties: Fines up to EUR 5,000,000.
Poland	Article 73 of the National Cybersecurity Act of 5 July 2018.	Administrative Penalties: Fines up to PLN 1,000,000 (approx. EUR 230,000)
Portugal	Articles 23 and 24 of Law No 46/2018 of 13 August 2007 establishing the legal framework for the security of cyberspace, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures to ensure a high common level of network and information security across the Union.	Administrative Penalties: • *Very serious infractions:* fines from EUR 5,000 up to 25,000 to individuals and from EUR 10,000 up to 50,000 to legal entities. • *Serious infractions:* fines from EUR 1,000 up to 3,000 to individuals and EUR 3,000 to 9,000 to legal entities.
Romania	Article 39 of Law no. 362/2018 ensuring a high common level of security of network and information systems.	Administrative Penalties: Fines from RON 3,000 (approx. EUR 670) to 50,000 (approx. from EUR 670 up to 11,000). Repeated breaches of the obligations may be sanctioned with administrative fines of up to RON 100,000 (approx. EUR 22,000). In case of companies with a turnover exceeding RON

Country	Applicable legal provisions	Penalties
		2,000,000 (approx. EUR 440,000), the administrative fines may be of up to 2% of the company's turnover and, for repeated breaches, of up to 5% of the company's turnover.
SLOVAKIA	Articles 30 and 31 of Act No 69/2018 on cybersecurity and amending certain acts.	Criminal penalties (offences): Fines from EUR 100 up to 5,000 to individuals.
		Administrative penalties: Fines from EUR 300 up to 1% from the total annual turnover but not exceeding EUR 300,000 to legal entities. In case of repeated violations the applicable fines can be doubled.
SLOVENIA	Articles 36, 37, 38, 39 of the Information Security Act.	Criminal Penalties (minor offences): • Fines from EUR 500 up to 10,000 to legal entities, and from EUR 10,000 up to 50,000 to medium-size or large companies • Fines from EUR 500 up to 10,000 to individuals or sole proprietors. • Fines from EUR 200 up to 2,000 to the responsible person of a legal entity, of a sole proprietor, of a self-employed person and of a state body, self-governing local community or in any other party governed by public law.
SPAIN	Title VII of the Royal-Decree-Law 12/2018 of 7 September on Security of Network and Information Systems.	Administrative Penalties: • *Very serious offences*: fines from EUR 500,001 up to 1,000,000. • *Serious offences:* fines from EUR 100,001 up to 500,000. • *Minor offences:* warnings or fines up to EUR 100,000.
SWEDEN	Sections 28, 29 and 30 of the Law (2018:1174) on Information Security for Essential and Digital Services.	Administrative penalties: Fines from SEK 5,000 up to 10,000,000 (approx. from EUR 500 up to 950,000).
UNITED KINGDOM	Section 18 of the Network and Information Systems Regulations 2018.	Administrative penalties: Fines up to GBP 17,000,000 (approx. EUR 20,000,000).

Overview penalties under the national transposition measures of the NIS Directive as of September 2022

In addition, the subsequent table provides an overview of the severity of fines highlighting the discrepancies across the European Union.



Overview severity of fines as of September 2022

III. Review of the NIS Directive

According to the Study to Support the Review of the NIS Directive (European Commission et al., 'Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665, Final Study Report', p. 16 and 89) two issues arise in terms of national penalties regimes: their great variation in characteristics and magnitude across Members States and their application. Regarding the magnitude, in some cases the penalties are almost not existent, while in some others they vary ten times as much. Generally, differences in characteristics and magnitude of penalties have not been identified as a key priority to be addressed in the context of the NIS Directive review but their misalignment can lead operators with cross borders activities to adopt a strategy of 'opportunity shopping' by notifying in the state with a lower penalty.. In addition, many Member States have not applied any penalty at the time of the evaluation supporting the Study to Support the Review of the NIS Directive. Although convergence in applying penalties is not a key priority in the current NIS Directive, a weak application of sanctions on non-compliance may result in suboptimal levels of cybersecurity at EU level, considering the cross-border dimension of it.

IV. Outlook: The NIS 2 Directive

In the Explanatory Memorandum of the NIS 2.0 Proposal, the Commission concludes that the supervision and enforcement regime of the NIS Directive is ineffective. In this sense, the Commission points out that Member States have been very reluctant to apply penalties to entities failing to put in place security requirements or report incidents and it warns that this can have negative consequences for the cyber resilience of individual entities.

The NIS 2 Proposal provided that Member States can decide to impose penalties of administrative and criminal nature, and to increase harmonisation it establishes a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations. These sanctions include binding instructions, an order to implement the recommendations of a security audit, an order to bring security measures into line with NIS requirements, and administrative fines (up to €10 million or 2 % of the entities' total turnover worldwide, whichever is higher). Furthermore, the Proposal specified that the national competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity and the imposition of a temporary ban from the exercise of managerial functions by a natural person and clarifies that given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied as ultima ratio. These provisions are enshrined in Chapter VII on supervision and enforcement of the NIS 2 Directive.

While the provision on penalties in Article 36 NIS 2 Directive only requires Member States to lay down rules on penalties, Article 32(7) NIS 2 Directive determines factors to be

considered when taking the aforementioned enforcement measures (which are set forth in Article 32(4) and (5) NIS 2 Directive). Taking into account the circumstances of each individual case, the competent authorities must consider inter alia the seriousness of the infringement, its duration, and the damage caused or losses incurred or potential damage or losses that could have been triggered.