Security and incident reporting requirements

Dumortier, Franck

Published in:
Electronic communications, audiovisual services and the internet

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

CHAPTER VI

SECURITY AND INCIDENT REPORTING REQUIREMENTS

Franck Dumortier

A. INTRODUCTION

Introduction In the current context of Big Data, cloud computing, Internet of Things (IoT) and more generally the upward interconnection of IT systems, information security has moved from the sole technical field to become a key legal issue, not only to ensure the effectiveness of the fundamental rights to privacy[1] and the protection of personal data[2] but also to improve the functioning of the internal market by creating trust and confidence. Both the General Data Protection Regulation[3] ("GDPR") and the Directive on security of network and information systems[4] ("NIS Directive") impose risk-based security measures and incident reporting obligations to warrant confidentiality, integrity and availability[5] of information but their objectives are different: whereas the GDPR aims to safeguard the processing of personal data, the NIS Directive is focused on the resilience of networks and IT systems which play a vital role in society. Consequently, under the GDPR, security and incident reporting requirements depend on the risk for the rights and freedoms of natural persons whereas, under the NIS Directive, these obligations depend on the risk for the continuity of services which are considered to be essential to economic and societal activities. Given the broad definition of personal data,[6] the organisations which must respect the provisions of the NIS Directive often also have to comply with the GDPR requirements.[7] In parallel to these two pieces of legisla- **6-001**

---

1 In *I v Finland* (Application no.20511/03), [2008] CE:ECHR:2008:0717JUD002051103, the European Court of Human Rights decided that art.8, §1 of the European Convention of Human Rights implies practical and effective protection to exclude any possibility of unauthorised access to personal data.

2 For aspects relating to privacy and data protection, see Chapter V.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 ("GDPR").

4 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 [2016] OJ L194/1 ("Directive on security of network and information systems").

5 The ISO/IEC 27000 family—which is the most known and widely employed standard in the area of information security—is based on the CIA triad (confidentiality, integrity, availability).

6 Recital 30 of the GDPR specifies that even online identifiers can be considered personal data, which would seem to include in some instances IP addresses. In *Patrick Breyer v Bundesrepublik Deutschland* (C-582/14) EU:C:2016:930, the Court decided that dynamic IP addresses can constitute personal data. See also Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP136 (20 June 2007). The concept of personal data is further discussed in para.5-011.

7 Directive on security of network and information systems art. 2.

tion, telecom providers are subject to a specific regime[8] and the NIS Directive does not apply to undertakings targeted by EU sector-specific legislation imposing security and notification requirements, such as the eIDAS Regulation[9] and the revised Payment Service Directive.[10] Additionally, the Cybersecurity Act[11] provides for a new certification framework for ICT processes, products and services, together with a stronger role for the EU Cybersecurity Agency ("ENISA").

6-002 **General Data Protection Regulation** The GDPR, which replaces the 20-year-old Data Protection Directive 95/46/EC,[12] is directly applicable in all Member States from 25 May 2018.[13] Where a processing of personal data falls within the territorial scope of the GDPR,[14] one of the core obligations of both data controllers and data processors[15] is to set up appropriate technical and organisational measures to ensure a level of security appropriate to the risk "to the rights and freedoms of natural persons".[16] When such a risk is susceptible to being high, the data controller is accountable to conduct a data protection impact assessment before starting the processing.[17] Furthermore, the Regulation lays down a set of rules on personal data breaches by introducing an obligation to notify the supervisory authority at the latest within 72 hours from when the data breach is likely to pose a risk to an individual's rights and freedoms.[18] In addition, when the personal data breach is likely to result in such a high risk, there is an obligation to inform the person whose data is concerned by the breach.[19]

6-003 **Directive on security of network and information systems** The NIS Directive which entered into force in August 2016 is the first EU horizontal legislation addressing cybersecurity challenges in Europe. Member States had to transpose the

8 See from paras 5-005, 5-067.

9 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 L275/73 ("eIDAS Regulation").

10 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 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 ("Revised Payment Service Directive").

11 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) no.526/2013 ("Cybersecurity Act").

12 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 L281/38 ("Directive 95/46/EC").

13 GDPR is discussed in paras 5-004, 5-009 and onwards.

14 "GDPR art.3" defines the territorial scope of the Regulation on the basis of two main criteria: the "establishment" criterion, as per art.3(1), and the "targeting" criterion as per art.3(2). Where one of these two criteria is met, the relevant provisions of the GDPR will apply to the processing of personal data by the controller or processor concerned. In addition, art.3(3) confirms the application of the GDPR to the processing where Member State law applies by virtue of public international law. About the territorial scope, see European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)", draft for public consultation (16 November 2018). See also para.5-010.

15 These concepts have been analysed in Article 29 Data Protection Working Party, Opinion 1/2010 on the concept of "controller" and "processor", WP169 (16 February 2010). See also para.5-012.

16 GDPR art.32.1. See also para.5-020.

17 GDPR art.35.1. See also para.5-028.

18 GDPR art.33. See also para.5-029.

19 GDPR art.34.

requirements of the Directive into their own national laws by 9 May 2018.[20] The aim of the NIS Directive is to boost the overall level of cybersecurity in the EU by requiring Member States to adopt a national strategy on the security of network and information systems, creating a Cooperation Group in order to support and facilitate strategic cooperation, and requiring Member States to designate national competent authorities, single points of contact and Computer Security Incident Response Teams (CSIRTs).[21] Moreover, the Directive establishes security and notification requirements for operators of essential services ("OESs") and digital service providers ("DSPs"). Although the Directive defines the types of DSPs falling in its scope (online marketplaces, online search engines and cloud computing services[22] when these types of services are not offered by micro- and small enterprises[23]), each Member State is responsible for identifying the OESs established in their territories. The following must be identified as an OES: (i) any public or private entity which provides a service which is essential for the maintenance of critical societal and/or economic activities in the sectors[24] of energy (e.g., electricity, oil and gas companies), transportation (including air, rail, water and road transport), healthcare (like hospitals and private clinics), certain banking and finance institutions (such as credit), suppliers and distributors of drinking water, and digital infrastructure (internet exchange points, domain name service providers and top level domain name registries); (ii) which depends on network and information systems; and (iii) on which an incident would have significant disruptive effects.[25] Both the OESs and the DSPs must take appropriate and proportionate technical and organisational measures to manage risks and prevent incidents affecting the security of their network and information systems and notify competent national authorities of security incidents of particular magnitudes, calculated in terms such as the number of users affected, the duration of the incident or the geographical spread with regard to the area affected by the incident.[26]

6-004 **Cybersecurity Act** The Regulation containing the Cybersecurity Act focuses on two key elements. Firstly, it replaces the previous ENISA Regulation[27] with the aim to create a permanent mandate[28] for the EU cybersecurity agency. The objective is to increase the agency's financial and human resources in order to ensure that ENISA cannot only provide expert advice, as has been the case until now, but can also perform operational tasks, notably to ensure effective and coordinated responses at Union level in the case of large-scale cross border incidents. Secondly, the Regulation provides for a voluntary European cybersecurity certification framework to encourage ICT products, services and processes being sold in EU countries to comply with cybersecurity standards. Indeed, while an increasing

20 Directive on security of network and information systems art.25.

21 Directive on security of network and information systems art.1.2.

22 The types of DSPs are listed in Annex III of the Directive on security of network and information systems.

23 Directive on security of network and information systems art.16.11.

24 Each sector and subsector covered is listed in Annex II of the Directive on security of network and information systems.

25 Directive on security of network and information systems art.5.2.

26 Directive on security of network and information systems arts 14 to 16.

27 Regulation (EU) No.526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No.460/2004 [2013] OJ L165/41.

28 The agency was established for a period of seven years beginning on 19 June 2013 and its mandate would therefore have ended in June 2020.

number of devices is connected to the internet, security and resilience are not always sufficiently built in by design. The Digital Single Market, and in particular the data economy and the IoT, can thrive only if there is general public trust that such products, services and processes provide a certain level of cybersecurity. Therefore, the Cybersecurity Act contains rules governing European cybersecurity certification schemes allowing certificates issued under those schemes to be valid and recognised across all Member States and addressing the current market fragmentation.

B. SECURITY OF PERSONAL DATA (GDPR)

1. Principles and allocation of responsibilities

6-005 **The principle of integrity and confidentiality** The GDPR establishes the principle of "integrity and confidentiality" of personal data at the same level as the traditional data quality principles (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation).[29] According to this principle, personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[30] Unlike the properties of integrity and confidentiality, the property of availability is not expressly mentioned in art.5.1(f). Nonetheless, the Article 29 Working Party—which is now replaced by the European Data Protection Board ("EDPB")[31]—considers that personal data breaches can be categorised according to the three information security properties as follows: (1) "confidentiality breach", where there is an unauthorised or accidental disclosure of, or access to, personal data; (2) "integrity breach" where there is an unauthorised or accidental alteration of personal data; and (3) "availability breach" where there is an accidental or unauthorised loss of access to, or destruction of, personal data.[32] This leads ENISA to consider that, under the GDPR, the security principle equally covers confidentiality, integrity and availability.[33]

29 Under Directive 95/46/EC, the security principle was not listed amongst the principles relating to data quality. However, its art.17 already imposed the security duty to both the data controller and the data processor.

30 GDPR art.5.1(f). See also Chapter V (para.5-020).

31 This Working Party was set up under art.29 of the Directive 1995/46/EC as an EU advising body with specific tasks. The Party consisted of a representative of the national data protection authorities, of the EU Commission and of the European Data Protection Supervisor. This Working Party is transformed under the GDPR into the European Data Protection Board ("EDPB"). See also para.5-038.

32 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01 (6 February 2018), p.7.

33 ENISA, Guidelines for SMEs on the security of personal data processing (December 2016), p.7.

6-006 **Allocation of roles, security and accountability** For both the data controller[34] and the data processor,[35] one of the core obligations under the GDPR is that of the security of personal data. Accordingly, the two actors[36] are required to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk "to the rights and freedoms of natural persons" posed to the personal data being processed[37] and provide a general description of these measures, where possible, in their records of processing activities.[38] In comparison with the data processor, the data controller has an additional duty of accountability according to which they are obliged to implement appropriate and effective measures, and be able to demonstrate compliance with the Regulation of processing activities carried out by the controller or on the controller's behalf, including the effectiveness of the measures.[39] This accountability requirement includes two elements: the need for data controllers to implement real and effective policies, procedures and mechanisms to safeguard the protection of individuals' information, as well as the obligation to maintain evidence in order to prove this should data protection authorities request it.[40] In practice, this additional accountability obligation consists in carrying out a data protection impact assessment ("DPIA"), to identify where a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons".[41] Clarifying the roles also has an impact on the confidentiality rule enshrined in art.29 of the GDPR according to which the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process that data except on instructions from the controller, unless required to do so by Union or Member State law.

6-007 **Joint-controllership** Where a controller determines the purposes and means of the processing jointly with other controllers, the liability of the joint controllers requires a clear and transparent allocation of their responsibilities by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.[42] In addition to a precise definition of their respective obligations, the arrangement must duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and may designate a contact point for them. However, irrespective of the terms of the arrangement, the data subject may exercise his or her rights in respect of and against each of the controllers.[43] In cases in which their processing requires a DPIA, the arrangement should set out which party is responsible for the various measures designed to treat risks and to protect

34 The "controller" is defined in art.4(7) of the GDPR as being "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

35 The "processor" is defined in art.4(8) of the GDPR as being "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

36 The concepts of controller and processor are discussed in para.5-012.

37 GDPR art.32.1.

38 GDPR arts 30.1(g) and 30.2(d).

39 GDPR arts 5.1(f), 24 and recital 74.

40 Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173 (13 July 2010), p.5.

41 GDPR art.35.1.

42 GDPR art.26.1 and recital 79.

43 GDPR arts 26.1 and 26.2.

the rights and freedoms of the data subjects. Each data controller should express their needs and share useful information without either compromising secrets (e.g. protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.[44] Furthermore, the EDPB recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.[45]

6-008 **Processing on behalf of a controller** Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures, including for the security of the processing.[46] In order to warrant appropriate safeguards, processing by a processor must be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.[47] The contract must also contain minimum terms requiring, amongst others, the processor to only act on the written instructions of the controller; ensure that persons authorised to process personal data are subject to a duty of confidence; take appropriate measures to ensure the security of processing; assist the controller in meeting its own obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments; submit to audits and inspections and provide the controller with whatever information it needs to ensure that they are both meeting their contractual obligations.[48] Furthermore, where a processor wants to engage a sub-processor for carrying out specific processing activities on behalf of the controller, this may not be done without prior specific or general written authorisation of the controller[49] and the same data security obligations as set out in the contract between the controller and the processor must be contractually imposed on that sub-processor.[50] In case the sub-processor fails to fulfil its data protection obligations, the initial processor remains fully liable to the controller for the performance of that other processor's obligations.

6-009 **Allocation of roles and liability** Any person who has suffered material or non-material damage as a result of a security breach has the right to receive compensation either from the (joint) controller or processor for the damage suffered.[51] In order to ensure effective compensation of the data subject, the GDPR institutes a cumulative liability regime in the sense that where controllers and processors are involved in the same processing and are responsible for any damage caused by a security breach, each shall be held liable for the entire damage.[52] However, a processor or controller that is held liable to pay compensation on this basis is entitled to recover from other relevant parties that part of the compensation corresponding to their part of the responsibility for the damage.[53] In this perspective, the allocation of roles between the data controller and the data processor has consequences on the liability exposure of the different actors involved in personal data processing operations.[54] Whereas any controller remains generally liable for any damages arising from the unlawful processing, the processor is only liable if they fail to comply with the obligations of the GDPR directed specifically to processors or if they acted outside or contrary to lawful instructions of the controller.[55] In case of a data breach, both actors can only be exempted from their liability if they prove they are not in any way responsible for the event giving rise to the damage.[56] Such evidence is not always easy to provide given that the duty of security enshrined in art.32 must be considered as an obligation of means—and not of result—according to which data controllers and data processors should act with the necessary degree of care and diligence to achieve an appropriate level of security. As a consequence of this categorisation, a debtor can only effectively avoid liability by demonstrating that they have selected and implemented every reasonable measure that might be expected from him to fulfil their obligation. Moreover detailed contractual clauses can bound a data processor or a (joint) controller by obligations of result, for example by imposing specific cryptographic algorithms, physical and logical access controls, or logging of processing operations. In such circumstances, one party can engage the liability of the other party more easily by merely demonstrating that the contractual result has not been achieved.

[44] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.7.

[45] Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (6 February 2018), p.13.

[46] GDPR art.28.1 and recital 81.

[47] GDPR art.28.3.

[48] GDPR art.28.3.

[49] GDPR art.28.2. In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

[50] GDPR art.28.4.

[51] GDPR art.82.1.

2. Evaluation of risks and appropriate security measures

6-010 **Evaluation of risks** A distinction must be made between "inherent" risk and "residual" risk. Inherent risk refers to the probability that a negative impact will occur when no protective action is taken. Residual risk refers to the probability that a negative impact will occur despite the measures taken to influence (or limit) the inherent risk.[57] Unlike risk management in information security—which is oriented towards the "assets"[58] of the organisation—the GDPR aims to manage risks "to the rights and freedoms of natural persons" which could lead to physical, material or

[52] GDPR art.82.4.

[53] GDPR art.82.5.

[54] See Van Alsenoy, B., *Regulating data protection. The allocation of responsibility and risk among actors involved in personal data processing*, Dissertation, 2016, p.610, available at *https://www.law.kuleuven.be/citip/en/staff-members/staff/00054907* [Accessed 16 September 2019].

[55] GDPR art.82.2.

[56] GDPR art.82.3.

[57] (French) Belgian Data Protection Authority, Recommandation d'initiative no.01/2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable (28 February 2018), pp.19–20.

[58] An information asset is a piece of data which has value to the organisation (e.g. an employee record, analysis reports, financial data of the organisation, etc.). See European Data Protection Supervisor, *Security Measures for Personal—Data Processing Article 22 of Regulation 45/2001* (21 March 2016), p.5.

non-material damages.[59] As indicated by the Article 29 Working Party, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.[60] Recital 75 of the GDPR provides for a non-exhaustive list of examples of potential negative impacts on data subject's rights: discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation,[61] situations where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data, or any other significant economic or social disadvantage. Article 32.2 of the GDPR identifies the threats which could lead to such risks. These threats consist, in particular, in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[62] As already mentioned, in addition to illegitimate access to data (loss of confidentiality), to unwanted modification of data (loss of integrity) and definitive unavailability of data, the Article 29 Working party also considers temporary unavailability of the processing, whether accidental (e.g. due to a power outage) or illicit (for example, following a "denial of service" attack)[63] as being an additional threat which could result in risks for data subjects' rights. The identified risks must be estimated in terms of severity and likelihood[64] which should be determined by reference to the nature, scope, context and purposes of the processing.[65] According to the French supervisory authority, severity represents the magnitude of a risk and primarily depends on the prejudicial nature of the potential impact; likelihood expresses the possibility of a risk occurring which depends on the level of vulnerabilities of the supporting assets when under threat and the level of capabilities of the risk sources to exploit them.[66] ENISA has issued guidelines for SMEs to assess security risks for personal data using an approach which is based on four steps, as follows: definition of the processing operation and its context,

[59] GDPR recital 75.

[60] Article 29 Working Party, Statement on the role of a risk-based approach to data protection legal frameworks, WP218 (30 May 2014), p.4.

[61] "Pseudonymisation" is defined in art.4(5) of the GDPR as "the processing of personal data in such a manner that the personal data can no.longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

[62] GDPR art.32.2.

[63] Distributed denial of service ("DDoS") attacks take advantage of the specific capacity limits that apply to any network resources—such as the infrastructure that enables a company's website. The DDoS attack will send multiple requests to the attacked web resource—with the aim of exceeding the website's capacity to handle multiple requests and prevent the website from functioning correctly.

[64] According to the French Supervisory Authority (CNIL), "a risk is a hypothetical scenario that describes a feared event and all the threats that would allow this to occur. More specifically, it describes: how risk sources (e.g.: an employee bribed by a competitor) could exploit the vulnerabilities of supporting assets (e.g.: the file management system that allows the manipulation of data) in a context of threats (e.g.: misuse by sending emails) and allow feared events to occur (e.g.: illegitimate access to personal data) on personal data (e.g.: customer file) thus generating impacts on the privacy of data subjects (e.g.: unwanted solicitations, feelings of invasion of privacy, personal or professional problems)". See CNIL, *Privacy Impact Assessment (PIA)—methodology* (February 2018), p.6.

[65] GDPR recital 76.

[66] CNIL, *Privacy Impact Assessment (PIA)—methodology* (February 2018), p.6.

understanding and evaluation of impact, definition of possible threats and evaluation of their likelihood (threat occurrence probability) and evaluation of risk (combining threat occurrence probability and impact).[67]

Selection of appropriate security measures The selection of appropriate security measures follows the "risk-based approach"[68] embodied by the GDPR according to which the higher the inherent risk, the more rigorous the security measures that the controller or the processor needs to take in order to reach an acceptable residual risk. After the evaluation of the inherent risk level and taking into account the state of the art[69] as well as the costs of implementation, the controller and the processor must implement technical and organisational measures to ensure a level of security appropriate to the risk.[70] The GDPR does not impose specific security measures but instead indicates that these may inter alia include, as appropriate, the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. National supervisory authorities provide more concrete guidance to implement appropriate security measures.[71] In addition, the controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.[72] Adherence to an approved code of conduct[73] or an approved certifica- **6-011**

[67] ENISA, Guidelines for SMEs on the security of personal data processing (December 2016). The Agency continued its activities in the area and focused on providing further guidance on the application of the aforementioned guidelines through specific uses cases. See ENISA, *Handbook on security of personal data processing* (December 2017).

[68] According to the Article 29 Working Party, "it is important to note that—even with the adoption of a risk-based approach—there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively 'low risk'. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk". See Article 29 Working Party, Statement on the role of a risk-based approach to data protection legal frameworks, WP218 (30 May 2014), p.2.

[69] TeleTrusT—IT Security Association Germany has written guidelines that are published in English in cooperation with ENISA about the meaning of "state of the art". TeleTrusT—IT Security Association Germany, *IT Security Act (Germany) and EU General Data Protection regulation—Guideline "State of the art"* (2019), available at *https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security* [Accessed 16 September 2019].

[70] GDPR art. 32.1.

[71] Examples are Belgian Data Protection Authority, Reference Measures for the Security of Any Personal Data Processing Operation, version 1.0, available at *https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/reference_measures_security_personal_data_processing_1.pdf* [Accessed 16 September 2019] and French Data Protection Authority (CNIL), *La sécurité des données personnelles—Les guides de la CNIL* (2018), available at *https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf* [Accessed 16 September 2019]

[72] GDPR art.32.4.

[73] As referred to in GDPR art.40.

tion mechanism[74] may be used as an element by which to demonstrate compliance with the security requirements.[75]

3. Data protection impact assessment

6-012 **Data protection impact assessment in case of a high risk** In line with the risk-based approach, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, data controllers must carry out a DPIA.[76] If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.[77] The GDPR provides three non-exhaustive examples of processing operations which are likely to result in an inherent high risk[78]: (i) a systematic[79] and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling,[80] and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (ii) processing on a large scale[81] of special categories of data[82] or of personal data relating to criminal convictions and offences;[83] or (iii) a systematic monitoring[84] of a publicly accessible area[85] on a large scale.

6-013 **Lists of processing operations requiring a DPIA** In order to provide a more

[74] As referred to in GDPR art.42.
[75] GDPR art.32.3.
[76] GDPR art.35.1.
[77] GDPR art.28.3(f).
[78] GDPR art.35.3.
[79] The Article 29 Working Party interprets "systematic" as "meaning one or more of the following: occurring according to a system; pre-arranged, organised or methodical; taking place as part of a general plan for data collection; carried out as part of a strategy". See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.10.
[80] According to art.4(4) of the GDPR, "profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".
[81] The Article 29 Working Party recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale: "the number of data subjects concerned either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity". See Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01 (5 April 2017), p.9.
[82] As referred to in art.9.1 of the GDPR.
[83] As referred to in art.10 of the GDPR.
[84] According to the Article 29 Working Party, "the concept of 'monitoring of the behaviour of data subjects' is mentioned in recital 24 and clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects". See Article 29 Working Party, Guidelines on Data Protection Officers ("DPOs"), WP243 rev.01 (5 April 2017), p.8.
[85] The Article 29 Working Party interprets "publicly accessible area" as being "any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library". See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.9.

concrete set of processing operations which are likely to result in a high risk, the national supervisory authorities ("SAs") must establish and make public a list of the kind of processing operations which are subject to the requirement for a DPIA.[86] Each national SA must communicate this draft list to the EDPB which is entitled to issue an opinion with the aim to apply the consistency mechanism as to avoid significant inconsistencies between EU Member States that may affect the equivalent protection of data subjects.[87] To support SAs in identifying when DPIAs are necessary, the Article 29 Working Party has issued Guidelines, endorsed by the EDPB, which set out a list of nine criteria to consider when identifying processing operations requiring a DPIA.[88] These criteria are met when processing involves evaluation or scoring including profiling and predicting; automated decision-making with legal or similar significant effect; systematic monitoring, sensitive data or data of a highly personal nature; data processed on a large scale; matching or combining datasets; data concerning vulnerable data subjects such as children, employees or the elderly; innovative use or applying new technological or organisational solutions; and preventing data subjects from exercising a right or using a service or contract. In most cases, a processing meeting two of those criteria would require a DPIA to be carried out, however, in some cases, a processing operation meeting only one of these criteria may require a DPIA, depending on the circumstances.[89] In line with those obligations, the SAs of 26 Member States submitted draft lists to the EDPB identifying data processing activities likely to result in a high risk and which therefore require DPIAs. The EDPB issued opinions on each of these lists, requesting that some SAs include certain types of processing in their lists, remove other types that the Board did not consider as creating high risks for data subjects, and use some criteria in a harmonised manner.[90]

6-014 **Content, scope and methodology of a DPIA** The GDPR does not formally define the concept of a DPIA as such, but specifies that it must contain at least a systematic description of the envisaged processing operations and the purposes of the processing; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance.[91] In accordance with the data protection by design and by default principles,[92] a DPIA should be carried out prior to the processing[93] and, as a matter of good practice, be continuously reviewed and

[86] GDPR art.35.4. Note that art.35.5 provides that SAs may also establish and make public a list of the kind of processing operations for which no DPIA is required. These lists must also be communicated to the EDPB.
[87] GDPR art.64.
[88] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017).
[89] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.11
[90] All of these opinions are on the website of the EDPB and available at *https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en* [Accessed 16 September 2019].
[91] GDPR art.35.7.
[92] GDPR art.25.
[93] GDPR arts 35.1 and 35.10, recitals 90 and 93. However, the requirement to carry out a DPIA ap-

regularly re-assessed.[94] The controller is ultimately responsible for ensuring that the DPIA is carried out, but the DPIA may be carried out by someone else, inside or outside of the organisation.[95] The controller must also seek the advice[96] of the Data Protection Officer[97] (DPO), where designated, and this advice, along with the decisions taken, should be documented within the DPIA.[98] Where appropriate, the controller is required to seek the view of data subjects.[99] It must document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.[100] A DPIA may concern a single data processing operation but could also be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose and risks. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided. The Article 29 Working Party encourages the development of sector-specific DPIA frameworks, so that the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies. The GDPR provides controllers with flexibility to determine the precise structure and form of the DPIA. Annex 1 of the Article 29 Working Party's Guidelines usefully sets out examples of existing EU DPIA frameworks, in Germany, Spain, France and the UK. Annex 2 further sets out criteria for an acceptable DPIA. Publishing a DPIA is not a legal requirement of the GDPR, and is at the controller's discretion. However, the Article 29 Working Party encourages the publication of DPIAs, as such a process would help foster trust in the controller's processing operations, and demonstrate accountability and transparency.[101]

6-015 **Prior consultation of the supervisory authority** Where a DPIA reveals a high residual risk which cannot be mitigated by appropriate measures in terms of available technology and costs of implementation, the data controller is required to seek prior consultation for the processing from the supervisory authority[102] which may provide its advice.[103] An example of an unacceptable high residual risk includes instances where, despite the envisaged security measures, the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g. by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not patched).[104] As part of this prior consultation, the DPIA must be fully provided.[105]

plies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing. See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.13.

94 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.14.

95 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017).

96 GDPR art.35.2.

97 GDPR art.37 indicates cases in which it is mandatory for certain controllers and processors to designate a DPO. Moreover, even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate one on a voluntary basis. See also Article 29 Working Party, Guidelines on Data Protection Officers ("DPOs"), WP243 rev.01 (5 April 2017). See also para.5-027.

98 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), pp.14-15.

99 GDPR art.35.9.

100 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.15.

101 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.18.

4. Notification and communication of security breaches

Notification of personal data breaches The GDPR requires the controller to notify any personal data breach to the supervisory authority unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. An example of this exemption might be where personal data is already publically available and a disclosure of such data does not constitute a likely risk to the individual.[106] The Article 29 Working Party considers that a controller should be regarded as having become "aware" when they have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.[107] Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach.[108] The notification must, at least, describe the nature of the personal data breach including where possible, the categories and approximate **6-016**

102 GDPR art.36.1 and recital 84.

103 GDPR art.36.2.

104 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.19.

105 GDPR art.36.3(e).

106 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (6 February 2018), pp.18-19. According to the Article 29 Working Party, this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.

107 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), pp.10-11. According to the Article 29 Working Party, "when, exactly, a controller can be considered to be 'aware' of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required".

108 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.23. According to the Article 29 Working Party, "it should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a

number of data subjects concerned and the categories and approximate number of personal data records concerned; communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; describe the likely consequences of the personal data breach; and describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[109] Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Nevertheless, as full and comprehensive details of the incident may not always be available during this initial period, notification in phases is allowed,[110] providing the controller gives reasons for the delay.[111] If a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, they must notify the controller "without undue delay".[112] However, the contract between the controller and processor could include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.[113] It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller: a processor just needs to establish whether a breach has occurred and then notify the controller.[114]

6-017 **Communication of personal data breaches** When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in addition to notifying the supervisory authority, the controller is also required to communicate the breach to the affected individuals.[115] The threshold for communicating a breach to individuals is higher than for notifying supervisory authorities and not all notified breaches have to be communicated to individuals, thus protecting them from unnecessary notification fatigue. Article 29 Working Party provides a non-exhaustive list of examples of when a breach is likely to result in high risk to individuals and consequently, instances when a controller has to notify a breach to those affected.[116] The GDPR states that communication of a breach to individuals should be made "without undue delay",[117] which means as soon as possible. The main objective of communications to individuals is to provide timely and specific

different focus to the risk considered in a DPIA. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals".

109 GDPR art.33.3.

110 GDPR art.33.4.

111 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (6 February 2018), p.15.

112 GDPR art.33.2.

113 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (6 February 2018), p.13.

114 See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (4 October 2017), p.13.

115 GDPR art.34.1.

116 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (6 February 2018), pp.31–33.

117 GDPR art.34.1.

information about steps they should take to protect themselves, such as resetting passwords in the case where their access credentials have been compromised.[118]

6-018 **Exceptions to communications** There are three exemptions to the obligation to communicate data breaches to the individuals.[119] The first exemption relates to situations where the controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenisation. The second exemption appears when, immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. The last exemption to communicate data breaches to individuals appears when it would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.[120]

6-019 **Legitimate interest to ensure network and information security** The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security[121] (NIS) and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. Consequently, the consent of data subjects is not needed in such cases.[122] This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping denial of service attacks and damage to computer and electronic communication systems.[123] In the same way, the NIS Directive explicitly states that personal data is in many cases compromised as a result of NIS incidents. In this context, competent national NIS authorities and data protec-

118 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (6 February 2018), p.20.

119 GDPR art.34.3.

120 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (6 February 2018), p.22.

121 Recital 49 of the General Data Protection Regulation and art.4(2) of the Directive on security of network and information systems use the same definition of "security of network and information systems". See below, para 6-19.

122 Legal grounds for the personal data processing to be lawful are discussed in para.5-022.

123 GDPR recital 49.

tion authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from NIS incidents.[124]

C. SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS DIRECTIVE)

6-020 **Objectives of the NIS Directive** The "NIS Directive" defines a "network and information system" as being either an electronic communications network[125] or any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data including digital data stored, processed, retrieved or transmitted by these systems for the purposes of their operation, use, protection and maintenance.[126] The security of these systems consists in their ability 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.[127] In order to fulfil its objectives, the NIS Directive establishes security and notification requirements for two different types of players, which are considered as being of particular critical importance: operators of essential services (OESs) and digital service providers (DSPs). Moreover, at the national level, the NIS Directive lays down obligations for Member States to adopt a national strategy as well as to designate national competent authorities, single points of contact and computer security incident response teams (CSIRTs). In addition, at European level, the NIS Directive creates a Cooperation Group (NIS Cooperation Group) with a view to fostering mutual understanding of challenges related to the implementation of key provisions of the Directive as well as to facilitate strategic cybersecurity cooperation and information sharing among Member States.[128] In parallel, the Directive creates a CSIRTs network to build confidence between Member States and to boost operational cybersecurity cooperation.[129]

1. Identification of undertakings subject to security obligations

6-021 **Identification of operators of essential services** The NIS Directive does not define explicitly which particular entities are considered as OESs under its scope.

[124] Directive on security of network and information systems recital 63.

[125] The concept of "electronic communications network" is defined in art.2(1) of the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L321/36 as being "transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed".

[126] Directive on security of network and information systems art.4(1).

[127] Directive on security of network and information systems art.4(2).

[128] The NIS Cooperation Group, composed of representatives of Member States, the Commission and ENISA, has been established by art.11 of the Directive on security of network and information systems.

[129] The network of Computer Security Incident Response Teams (the CSIRTs Network), dedicated to sharing information about risks and ongoing threats and cooperating on specific cybersecurity incidents, is established under art.12 of the Directive on security of network and information systems which also defines its roles.

Instead, it provides criteria that Member States are required to apply in order to identify OESs.[130] In November 2018 and every two years thereafter, each Member State is required to submit to the European Commission a list of identified OESs with an establishment on its territory.[131] As a result of this assessment, all entities that fulfil the criteria detailed hereunder shall be identified as OESs and be subject to the security and notification obligations of art.14[132]: (i) as a first step, Member States should assess whether an entity of interest belongs to the following *sectors and subsectors* listed in Annex II of the Directive, which are considered instrumental to ensuring the proper functioning of the internal market: energy (electricity, oil and gas), transport (air, rail, water and road), banking (credit institutions), financial market infrastructures (trading venues, central counterparties), health (healthcare providers including hospitals and private clinics), water (drinking water supply and distribution) and digital infrastructure (internet exchange points, domain name system service providers, top level domain name registries);[133] (ii) as a second step, the entity which is subject to the identification needs to provide a service which is *essential* for the maintenance of the critical societal and/or economic activities.[134] When carrying out this assessment, Member States should take into account that one entity can provide both essential and non-essential services. This means that the security and notification requirements of the NIS Directive will apply to a certain operator only to the extent to which it provides essential services;[135] and (iii) thirdly, it should be clarified whether the provision of the essential service depends on network and information systems.[136] Hence, as a third step, the identification process requires the assessment of whether an incident, being defined as any event having an actual adverse effect on the security of network and information systems,[137] would have a *significant disruptive effect on the provision of the service*. In this context, if appropriate, the assessment should consider sector-specific factors[138] but also at least the following cross-sectorial factors: the number of users relying on the service provided by the entity concerned;

[130] The criteria for identifying OESs are set out in art.5.2 of the Directive on security of network and information systems.

[131] Directive on security of network and information systems arts 5.3 and 5.5.

[132] It should be outlined that when carrying out the identification process, Member States should not add additional criteria because this could narrow the number of identified OESs and jeopardise the minimum harmonisation for OESs enshrined in art.3 of the Directive on security of network and information systems.

[133] For most of the entities which belong to the "traditional sectors", EU legislation contains well developed definitions to which Annex II makes a reference. However, for the sector of digital infrastructure, listed under point 7 of Annex II (Internet Exchange Points, Domain Name Systems and Top-level domain name registries), this is not the case. Therefore, with the aim to clarify these definitions, the Commission provided detailed explanation in the Annex of its Communication of 13 September 2017. See Annex to the Communication from the Commission to the European Parliament and the Council, Making the most of NIS—towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017)476 final/2 (4 October 2017), pp.20–22.

[134] Directive on security of network and information systems art.5.2(a).

[135] Directive on security of network and information systems art.14.3.

[136] Directive on security of network and information systems art.5.2(b).

[137] Directive on security of network and information systems art.4(7).

[138] Directive on security of network and information systems art.6.2. With regard to the sector-specific factors, recital 28 provides some examples which could provide helpful guidance to national authorities: "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,

the dependency of other sectors referred to in Annex II on the service provided by that entity; the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; the market share of that entity; the geographic spread with regard to the area that could be affected by an incident; and 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.[139]

6-022 **Jurisdiction of Operators of Essential Services ("OESs")** For the purposes of identifying OESs, establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements, whereas the legal form of those arrangements should not be a determining factor.[140] This means that a Member State can have jurisdiction over an OES not only in cases where the operator has its head office on its territory but also in cases where the operator has for example a branch or other type of legal establishment. This has the consequence that several Member States in parallel could have jurisdiction over the same entity. Therefore, where an entity provides a service which is essential for the maintenance of critical societal and/or economic activities in more than one Member State, those Member States must consult each other before they take a decision on the identification of the OES.[141] The desired outcome of the consultation is that the involved national authorities exchange arguments and positions and ideally come to the same decision concerning the identification of the operator concerned. However, the NIS Directive does not preclude Member States reaching divergent conclusions whether a particular entity is identified as an OES or not.[142] In the Commission's view, Member States should strive to reach a consensus on these issues to avoid a situation that the same company is facing different legal status in various Member States. Divergence should remain exceptional e.g. when an entity determined as an OES in one Member State has a marginal and insignificant activity in another one.[143] In order to facilitate the Member States when taking informed decisions related to whether an operator is essential or not as well as to avoid unnecessary divergence or inconsistencies, the NIS Cooperation Group issued a reference document on modalities of the consultation process in cases with cross-border impact.[144]

6-023 **Definition of Digital Services Providers (DSPs)** The DSPs are the second category of entities included in the scope of the NIS Directive. These entities are

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."

139 Directive on security of network and information systems art.6.1.

140 Directive on security of network and information systems recital 21.

141 Directive on security of network and information systems art.5.4.

142 Recital 24 of the Directive on security of network and information systems mentions the possibility for Member States to request the assistance of the Cooperation Group in that matter.

143 Annex to the Communication from the Commission to the European Parliament and the Council, Making the most of NIS—towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017)476 final/2 (4 October 2017), p.30.

144 NIS Cooperation Group, *Identification of operators of essential services—Reference document on modalities of the consultation process in cases with cross-border impact*, Publication 07/2018 (July 2018).

considered to be important economic players due to the fact that they are used by many businesses for the provision of their own services, and a disruption of the digital service could have an impact on the key economic and societal activities.[145] Contrary to the OESs, the Directive does not require Member States to identify the DSPs. Therefore, the relevant obligations of the Directive, namely the security and notifications requirements set out in art.16 apply to all DSPs within its scope. A "digital service" is defined as being any Information Society service[146] which is of a type listed in Annex III of the NIS Directive. This Annex lists three specific types of services—online market place, online search engine and cloud computing service: (i) online market place is defined as a service that enables consumers and traders to conclude online sales or service contracts with traders, and it represents the final destination for the conclusion of those contracts.[147] For example, a provider such as eBay can be regarded as an online market place as it allows others to set up shops on its platform in order to make their products and services available online to consumers or businesses. Also, online application stores for distributions of applications and software are considered as falling under the definition of online market place because they allow app developers to sell or distribute their services to consumers or other businesses. In contrast, intermediaries to third-parties services such as Skyscanner and price comparison services, which redirect the user to the website of the trader where the actual contract for the service or the product is concluded, are not covered by the definition; (ii) online search engine is defined as a digital service that allows users to carry out searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject. Search functionalities limited to in-site search and price comparison websites are not covered, irrespective of whether the search function is provided by an external search engine;[148] and (iii) finally, cloud computing service is defined as a digital service that enables access to a scalable and elastic pool of shareable computing resources.[149] The term "scalable" refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term "elastic pool" is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term "shareable" is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.[150] When meeting these characteristics, the computing resources falling in the scope of the NIS Directive include resources such as networks, servers or other infrastructure, storage, applications and services. In other words, all current main types of cloud service models are targeted, such as Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS") and Software as a Service ("SaaS").

145 Directive on security of network and information systems, recital 48.

146 The concept of "Information Society service" is defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" in art.1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1.

147 Directive on security of network and information systems art.4(17) and recital 15.

148 Directive on security of network and information systems art.4(18) and recital 16.

149 Directive on security of network and information systems art.4(19).

150 Directive on security of network and information systems recital 17.

6-024 **Jurisdiction of DSPs** As regards the question of territoriality, the Directive takes into account the cross-border nature of DSPs and does not follow the model of multiple parallel jurisdictions but an approach which focuses on where a DSP is established in the Union; it will be subject to the jurisdiction of the Member State where it has its main establishment, which in principle corresponds to the place where the provider has its head office in the Union.[151] In cases where the concerned DSP offers services in the EU but is not established in the EU territory, the NIS Directive imposes on the DSP the obligation to designate a representative in the Union. In that case, the Member State where the representative is established will have jurisdiction over the company.[152] In cases where a DSP provides services in a Member State but has not designated a representative in the EU, the Member State can in principle take actions against the DSP as the provider is infringing its obligations deriving from the Directive.[153] This approach allows for a single set of rules to be applied to DSPs with one competent authority responsible for supervision which is particularly important, as many DSPs offer their services across many Member States simultaneously. The application of this approach minimises the compliance burden on DSPs and ensures the proper functioning of the Digital Single Market.

2. Security obligations

6-025 **Security requirements of OESs** For what concerns OESs, Member States are required to ensure that, having regard to the state of art, the identified entities take appropriate and proportionate technical and organisational measures to manage the risk posed to the security of network and information systems which the organisations use in the provision of their services.[154] In this context, a risk means any reasonably identifiable circumstance or event having a potential adverse effect[155] on the security of network and information systems.[156] Furthermore, Member States must ensure that appropriate measures are taken to prevent and minimise the impact of an incident with a view to ensuring the continuity of those services.[157] In order to provide guidance to the Member States, the NIS Cooperation Group issued non-binding guidelines concerning the security measures for OESs.[158] As highlighted by the Commission, harmonisation of such requirements would greatly facilitate compliance by OESs which often provide essential services in more than one Member State and the supervision tasks of national competent authorities and CSIRTs.[159]

[151] Directive on security of network and information systems art.18.1 and recital 64.
[152] Directive on security of network and information systems art.18.2.
[153] Directive on security of network and information systems art.18.3.
[154] Directive on security of network and information systems art.14.1.
[155] "Adverse effect" is a concept not defined within the Directive on security of network and information systems. Nonetheless, the NIS Cooperation Group considers the general meaning of the words: preventing success or development, harmful, unfavourable. See NIS Cooperation Group, *Reference document on incident notification for operators of essential services—circumstances of notification*, Publication 02/2018 (February 2018), p.10.
[156] Directive on security of network and information systems art.4(9).
[157] Directive on security of network and information systems art.14.2.
[158] NIS Cooperation Group, *Reference document on security measures for Operators of Essential Services*, Publication 01/2018 (February 2018).
[159] Annex to the 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 (4 October 2017), p.30.

6-026 **Notification requirements of OESs** Additionally, Member States also have to ensure that OESs notify, without undue delay, the competent authority or the CSIRT regarding any incident that has a significant impact on the continuity of the essential services.[160] Given the already mentioned definition of the term "security of network and information systems", the Cooperation Group considers that any event affecting not only the availability but also the authenticity, integrity or confidentiality of networks and information systems (used in the provision of the essential service), that has a significant impact on the continuity of the essential service itself should trigger the notification obligation.[161] In order to determine the significance of the impact of an incident, the following parameters, in particular, must be taken into account: the number of users affected by the disruption of the essential service, the duration of the incident and the geographical spread with regard to the area affected by the incident.[162] When measuring the significance of incidents, each Member State may also decide industry specific parameters and thresholds, to reflect the reality within a sector or national particularities. A generic threshold can be set at national level (e.g. one million users affected), or different thresholds per industry (e.g. health: 100,000 patients affected, energy: one million users affected). In terms of parameters, Member States can measure significance of the impact by using only the three parameters mentioned above, using an extended generic set of parameters, besides the ones imposed by the Directive, or using sectoral sets of parameters, adapted to particularities within each sector/subsector.[163]

6-027 **Possible inclusion of additional sectors** Besides the mandatory security and notification requirements of the NIS Directive concerning OESs and taking into account the minimum harmonisation provision enshrined in art.3, Member States can adopt or maintain legislation ensuring a higher level of security of network and information systems. In this regard Member States are in general free to expand the security and notification obligations under art.14 to entities belonging to other sectors and sub-sectors than those listed in Annex II of the NIS Directive. Various Member States have decided to include some of the following additional sectors: public administrations, the postal sector, the food sector, the chemical and nuclear industry, the environmental sector and the civil protection sector.[164]

6-028 **Security requirements of DSPs** In the same logic as for OESs, Member States are required to ensure that DSPs take appropriate and proportionate technical and organisational measures to manage the risk posed to the security of network and information systems which the companies use in the provision of their services. Those security measures should take into account the state of the art and the fol-

[160] Directive on security of network and information systems art.14.3.
[161] NIS Cooperation Group, *Reference document on incident notification for operators of essential services—circumstances of notification*, Publication 02/2018 (February 2018), p.10. The same applies to DSPs.
[162] Directive on security of network and information systems art.14.4.
[163] NIS Cooperation Group, *Reference document on incident notification for operators of essential services—circumstances of notification*, Publication 02/2018 (February 2018), p.15.
[164] Annex to the Communication from the Commission to the European Parliament and the Council, Making the most of NIS—towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017)476 final/2 (4 October 2017), pp.23–24.

lowing five elements: security of systems and facilities; incident handling; business continuity management; monitoring, auditing and testing; as well as compliance with international standards.[165] The Commission adopted an implementing Regulation which further specifies the elements to be taken into account by DSPs when identifying and taking measures to ensure a level of security of network and information systems which they use in the context of offering services referred to in Annex III.[166] Moreover, ENISA issued technical guidelines which define common baseline security objectives as well as different levels of sophistication in their implementation, mapping these against well-known industry standards, national frameworks and certification schemes.[167]

6-029 **Notification requirements of DSPs** DSPs have to take the necessary measures to prevent and minimise the impact of incidents with a view to ensuring the continuity of their services.[168] Hence, DSPs are required to notify the competent authority or the CSIRT, without undue delay, of any incident having a substantial impact on the provision of a service.[169] For determination of the impact, the NIS Directive lists five particular parameters that need to be taken into account: (i) the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (ii) the duration of the incident; (iii) the geographical spread with regard to the area affected by the incident; (iv) the extent of the disruption of the functioning of the service; and (v) the extent of the impact on economic and societal activities.[170] In the Implementing Regulation, the Commission further specifies the parameters to be taken into account to determine whether an incident has a substantial impact on the provision of those services.[171] As an exemption, DSPs which are micro or small enterprises within the meaning of Commission Recommendation 2003/361/EC[172] are excluded from the scope of the security requirements and notification.[173] This means those businesses that employ fewer than 50 persons and which have an annual turnover and/or an annual balance sheet total not exceeding €10 million, are not bound by such requirements. When determining the size of the entity, it is not of relevance whether the company concerned provides only digital services within the meaning of the NIS Directive or also other services. Moreover, Member States are not allowed to impose any further security and notification requirements on DSPs than those provided in the Directive, except for cases where such measures are necessary to safeguard their essential State functions, in particular to safeguard national security, and to allow

[165] Directive on security of network and information systems art.16.1.

[166] 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 ("Commission Implementing Regulation 2018/151") art.2.

[167] ENISA, *Technical Guidelines for the implementation of minimum security measures for digital service providers* (December 2016).

[168] Directive on security of network and information systems art.16.2.

[169] Directive on security of network and information systems art.16.3.

[170] Directive on security of network and information systems art.16.4.

[171] Commission Implementing Regulation 2018/151 arts 3 and 4.

[172] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L124 ("Commission Recommendation 2003/361/EC").

[173] Directive on security of network and information systems art.16.11.

for the investigation, detection and prosecution of criminal offences.[174] Finally, it should be highlighted that a DSP is only subject to a light-touch and reactive ex post supervisory control by the national competent authorities.[175] The competent authority concerned should therefore only take action when provided with evidence, for example by the DSP itself, by another competent authority, including a competent authority of another Member State, or by a user of the service, that a DSP is not complying with the security and notification requirements, in particular following the occurrence of an incident.[176]

6-030 **National NIS strategy** All Member States need to adopt a national strategy on the security of network and information systems ("NIS strategy") defining the objectives and appropriate policy and regulatory measures.[177] This strategy should include strategic objectives, priorities and a governance framework; identification of measures on preparedness, response and recovery; cooperation methods between the public and private sectors; awareness raising, training and education; research and development plans related to the NIS strategy, a risk assessment plan as well as a list of actors involved in the strategy implementation. Pursuant to the wording of art.7, the obligation to adopt an NIS strategy only applies to the sectors referred to in Annex II (types of OESs) and to the services referred to in Annex III (types of DSPs). However, art.3 of the NIS Directive specifically sets forth the principle of minimum harmonisation, pursuant to which Member States may adopt or maintain provision with a view to achieving a higher level of security of network of information systems. The application of this principle to the obligation to adopt an NIS strategy enables Member States to include more sectors and services than the aforementioned ones, for example to include public administrations responsible for sensitive sectors and services other than those listed in the Directive's Annexes II and III, which warrant the need of being covered by an NIS strategy, as well as management plans preventing leaks and ensuring adequate protection.

3. Institutions

6-031 **National competent authorities** In order to monitor the application of the Directive at national level and to assess compliance of OESs and DSPs with their obligations, art.8 requires Member States to designate national competent authorities on security of networks and information systems, while explicitly recognising the possibility to designate "one or more national competent authorities".[178] Accordingly, Member States are free to choose to designate one single authority dealing with all sectors and services covered by the Directive or several authorities, depending for example on the type of sector. When deciding on the approach, Member States can

[174] Directive on security of network and information systems art.16.10.

[175] Directive on security of network and information systems art.17.1.

[176] Directive on security of network and information systems recital 60.

[177] Directive on security of network and information systems art.7.

[178] Recital 30 of the Directive on security of network and information systems explains this policy choice: "In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks link to the security of the network and information systems of operators of essential services and digital service providers under this Directive."

draw on the experience from the national approaches used in the context of the existing legislation on critical infrastructure protection.[179]

6-032 **Computer Security Incident Response Team(s) ("CSIRT")** Additionally, Member States need to appoint at least one CSIRT[180] entrusted with the task of handling risks and incidents for the types of OESs and DSPs listed in the NIS Directive's Annexes II and III. Member States can opt for establishing a CSIRT within the national competent authority(ies). Taking into account the minimum harmonisation requirement enshrined in art.3 of the Directive, Member States are free to use the CSIRTs also for other sectors not covered by the Directive, such as the public administration. The tasks of designated CSIRTs include monitoring incidents at a national level; providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents; responding to incidents; providing dynamic risk and incident analysis and situational awareness; and participating in the network of the national CSIRTs (CSIRTs network) established under art.12.[181] Specific additional tasks relate to incident notifications where a Member State decides that CSIRTs, in addition to or instead of national competent authorities, can undertake such roles.[182]

6-033 **National single point of contact** Finally, each Member State must designate a national single point of contact, which will exercise a liaison function to ensure cross-border cooperation with the relevant authorities in other Member States and with the NIS Cooperation Group and the CSIRT network.[183] This is particularly needed given that Member States may decide to have more than one national authority. Furthermore, Member States need to ensure that the single point of contact is informed about the received notifications from operators of essential services and digital service providers.[184]

D. EU CYBERSECURITY AGENCY AND EUROPEAN CERTIFICATION (CYBERSECURITY ACT)

6-034 **Objectives** Whereas ENISA previously had a limited mandate that would have ended in 2020, the first key objective of the Cybersecurity Act is to give the agency a permanent role as the EU agency for cybersecurity. Among its new tasks, ENISA will contribute to increase cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.[185] The Regulation also creates a voluntary European cybersecurity certification framework for ICT products,[186]

[179] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75.
[180] Directive on security of network and information systems art.9.
[181] Directive on security of network and information systems art.9 and Annex I.
[182] Directive on security of network and information systems arts 14.3, 14.5, 14.6, 16.3, 16.6 and 16.7.
[183] Directive on security of network and information systems art.8.
[184] Directive on security of network and information systems art.10.3.
[185] Cybersecurity Act arts 4.5 and 7.
[186] Cybersecurity Act art.2(12) defines an "ICT"product as "any element or group of elements of network and information systems".

services[187] and processes.[188] The reason is that many EU Member States have already developed and adopted national cybersecurity certification schemes but these are only recognised at national level, having little or no value outside their countries. Therefore, the Regulation contains rules governing European cybersecurity certification schemes allowing certificates issued under those schemes to be valid and recognised across all Member States.

1. The EU Cybersecurity Agency (ENISA)

ENISA's structure The administrative and management structure of ENISA is composed of a Management Board, an Executive Board, an Executive Director, an ENISA Advisory Group and a National Liaison Officers Network.[189] The Management Board is composed of one member appointed by each Member State and two members appointed by the Commission. All members are appointed for a renewable term of fours years on the basis of their knowledge in the field of cybersecurity and have the right to vote.[190] The Management Board establishes the general direction of ENISA's operations and is entrusted with the powers necessary to establish the budget, verify the execution of the budget, adopt appropriate financial rules, establish transparent working procedures for decision making, adopt ENISA's work programme, adopt its own rules of procedure, appoint the Executive Director and decide on the extension and termination of the Executive Director's term of office.[191] In order to prepare its decisions, the Management Board is assisted by an Executive Board composed of five members appointed from among the members of the Management Board.[192] To ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders on issues related to the annual work programme, the ENISA Advisory Group is established by the Management Board. The ENISA Advisory Group is composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, academic experts in the field of cybersecurity, and representatives of competent authorities in the field of electronic communications, of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities.[193] Finally, the National Liaison Officers Network is composed of representatives of all Member States (National Liaison Officers) to facilitate the exchange of information between ENISA and the Member States, and to support ENISA in disseminating its activities, findings and recommendations to the relevant stakeholders across the Union.[194] 6-035

ENISA's tasks under the Cybersecurity Act The Cybersecurity Act aims to reinforce ENISA's role as the EU's centre of advice and expertise with regard to 6-036

[187] Cybersecurity Act art.2(13) defines an "ICT service" as "any service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems".
[188] Cybersecurity Act art.2(14) defines an "ICT process" as "any set of activities performed to design, develop, deliver or maintain an ICT product or service".
[189] Cybersecurity Act art.13.
[190] Cybersecurity Act art.14.
[191] Cybersecurity Act art.15.
[192] Cybersecurity Act art.19.
[193] Cybersecurity Act art.21.
[194] Cybersecurity Act art.23.

cybersecurity matters.[195] A first task assigned to the agency is to contribute to the development and implementation of Union policy and law in the field of cybersecurity. To that end ENISA will, in particular, issue opinions and guidelines, develop best practices and assist Member States and EU institutions, bodies, offices and agencies in developing and promoting cybersecurity policies.[196] A second task of ENISA is to promote capacity-building by assisting Member States in preventing, detecting and improving their responsiveness to cyber threats and incidents by providing them with knowledge and expertise as well as by establishing and implementing vulnerability disclosure policies on a voluntary basis. In that context, ENISA must also support the exchange of information between sectors by providing best practices and guidance on available tools and procedures, as well as on how to address regulatory issues related to information-sharing.[197] A third major task of the agency is to analyse emerging technologies, provide topic-specific assessments on the expected impact of technological innovations on cybersecurity, and perform long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents. Through a dedicated portal, ENISA must make its findings available to the public and compile reports in order to provide guidance to citizens, organisations and businesses across the Union.[198] This task is related to the more general objective of ENISA to raise public awareness of cybersecurity risks by providing good practices, including in the fields of cyber-hygiene and cyber-literacy,[199] and advice on research needs and priorities in the field of cybersecurity.[200] Furthermore, the agency must promote international cooperation on issues related to cybersecurity by working with third countries and international organisations or within relevant international cooperation frameworks.[201] More fundamentally, the new missions of ENISA also include an increased operational cooperation task at EU level, in particular in the context of large-scale cross-border incidents, as well as a support and promotion task with regard to the development and implementation of the cybersecurity certification framework established by Title III of the Cybersecurity Act.

6-037 **Coordinated response to large-scale cybersecurity incidents** On 13 September 2017, after the unprecedented WannaCry and NotPetya cyber-attacks, the Commission adopted a Recommendation on coordinated response to large-scale cybersecurity incidents and crises,[202] of which the Annex is known as "the Blueprint".[203] According to the Blueprint, a cybersecurity incident may be considered a crisis at Union level when the disruption caused by the incident is too extensive for a concerned Member State to handle on its own or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level. In order to implement the Blueprint, the NIS Cooperation Group identified a taxonomy to categorise causes and impact of large-scale cybersecurity incidents[204] which has been welcomed by the Council.[205] The taxonomy has two core parts: the nature of the incident, i.e. the underlying cause that triggered the incident, and the impact of the incident, i.e. the impact on services, in which sector(s) of economy and society. In such cases, the Blueprint describes how well-established crisis management mechanisms should make full use of existing cybersecurity entities at EU level as well as of cooperation mechanisms between the Member States. In doing so, the Blueprint takes into account a set of guiding principles (proportionality, subsidiarity, complementarity and confidentiality of information), presents the core objectives of cooperation (effective response, shared situational awareness, public communication messages) at three levels (strategic/political, operational and technical), the mechanisms and the actors involved as well as the activities to meet said core objectives. The foundation of cooperation amongst Member States in responding to such incidents is provided by the CSIRTs Network established by the NIS Directive and of which the secretariat is provided by ENISA.[206]

[195] Cybersecurity Act art.3.
[196] Cybersecurity Act art.5.
[197] Cybersecurity Act art.6.
[198] Cybersecurity Act art.9.
[199] Cybersecurity Act art.10.
[200] Cybersecurity Act art.11.
[201] Cybersecurity Act art.12.
[202] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises [2017] OJ L239/36 ("Recommendation of 13 September 2017").
[203] Annex to the Recommendation of 13 September 2017 establishing a Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises [2017] OJ L239/36 ("the Blueprint").

ENISA's operational role increased at EU level The Cybersecurity Act consolidates the agency's operational role in the case of large-scale cross-border incidents by mandating ENISA to gather relevant information and act as a facilitator between the CSIRTs network and the technical community, as well as between decision makers responsible for crisis management. Furthermore, ENISA should support operational cooperation among Member States, where requested by one or more Member States, in the handling of incidents from a technical perspective, by facilitating relevant exchanges of technical solutions between Member States, and by providing input into public communications. ENISA should also support operational cooperation by testing the arrangements for such cooperation through regular cybersecurity exercises.[207] **6-038**

2. The EU cybersecurity certification framework

EU cybersecurity certification schemes Title III of the Regulation containing the Cybersecurity Act establishes a European cybersecurity certification framework in order to improve the conditions for the functioning of the internal market by enabling a harmonised approach to European cybersecurity certification schemes (hereafter "ECC schemes").[208] The aim of this framework is to attest that the ICT processes, products and services that have been evaluated in accordance with ECC schemes comply with specified security requirements. The objective of these schemes is to protect the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes and services throughout their life cycle.[209] A preliminary task of the Commission is to publish a Union "rolling work **6-039**

[204] NIS Cooperation Group, *Cybersecurity Incident Taxonomy*, Publication 04/2018 (July 2018).
[205] Council conclusions on EU coordinated response to large-scale cybersecurity incidents and crises, 10086/18, adopted by the General Affairs Council at its 3,629th meeting held on 26 June 2018.
[206] Directive on security of network and information systems art.12.
[207] Cybersecurity Act art.7 and recital 32.
[208] Cybersecurity Act art.46.1.
[209] Cybersecurity Act art.46.2.

programme"[210] for European cybersecurity certification that identifies strategic priorities for future ECC schemes and include a list of ICT products, services and processes or categories thereof that are capable of benefitting from being included in the scope of an ECC scheme.[211] The Union rolling work programme should allow industry, national authorities and standardisation bodies, in particular, to prepare in advance for future ECC schemes.[212] When a need is identified on the basis of the Union rolling work programme, the Commission may request ENISA to prepare a candidate scheme or to review an existing ECC scheme. Moreover, in duly justified cases, the Commission or the European cybersecurity certification group[213] (ECCG) may request ENISA to prepare a candidate scheme or to review an existing ECC scheme which is not included in the Union rolling work programme. The Union rolling work programme is then updated accordingly.[214] The candidate ECC schemes would be prepared by ENISA, after consultation of all relevant stakeholders[215] by means of a formal, open, transparent and inclusive consultation process and with the assistance, expert advice and close cooperation of the ECCG.[216] The Commission would then be empowered to adopt these ECC schemes by means of implementing acts. In principle, from the date established in the implementing act, national cybersecurity certification schemes and the related procedures for the ICT processes, products and services covered by a ECC scheme shall cease to produce effects.[217] Following the same logic, Member States shall not introduce new national cybersecurity certification schemes for ICT processes, products and services covered by a ECC scheme in force.[218] However, existing certificates that were issued under national cybersecurity certification schemes and are covered by an ECC scheme shall remain valid until their expiry date.[219] Of course, the specified requirements of the ECC schemes must be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law.[220] Furthermore, where a specific Union legal act so provides, a certificate or an EU

[210] According to art.47.5 of the Cybersecurity Act, the first Union rolling work programme shall be published 12 months after the entry into force of the Cybersecurity Act. The Union rolling work programme shall be updated at least once every three years and more often if necessary.

[211] Cybersecurity Act art.47. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof in the Union rolling work programme shall be justified on the basis of one or more of the following grounds specified in art.47.3 of the Cybersecurity Act.

[212] Cybersecurity Act recital 84.

[213] The ECCG is established by art.62 of the Cybersecurity Act. The ECCG shall be composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG shall not represent more than two Member States. Stakeholders and relevant third parties may be invited to attend meetings of the ECCG and to participate in its work.

[214] Cybersecurity Act art.48.

[215] A Stakeholder Cybersecurity Certification Group is established by art.22 of the Cybersecurity Act. The Stakeholder Cybersecurity Certification Group shall be composed of members representing industry in balanced proportions, both on the demand side and the supply side of ICT products and ICT services, and including, in particular, SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies, as well as academia and consumer organisations. The Commission, following a transparent and open call, shall select, on the basis of a proposal from ENISA, members of the Stakeholder Cybersecurity Certification Group ensuring a balance between the different stakeholder groups as well as an appropriate gender and geographical balance.

[216] Cybersecurity Act art.49.1.

[217] Cybersecurity Act art.57.

[218] Cybersecurity Act art.49.2.

[219] Cybersecurity Act art.49.3.

[220] Cybersecurity Act art.54.2.

statement of conformity issued under an ECC scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.[221]

Objectives of the certification schemes The adopted ECC schemes should be designed so as to achieve, as applicable, at least the following security objectives: to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure and against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, service or process; that authorised persons, programmes or machines are able only to access the data, services or functions to which their access rights refer; to identify and document known dependencies and vulnerabilities; to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities; to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident; that ICT products, ICT services and ICT processes are secure by default and by design and are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.[222] **6-040**

Content of the certification schemes The adopted ECC schemes should specify: (i) a minimum set of elements concerning, amongst others, their subject-matter and scope (including the type or categories of ICT processes, products and services covered); (ii) a clear description of the purpose of the scheme and of how the selected standards and evaluation methods correspond to the needs of the intended users of the scheme; (iii) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in the Regulation on standardisation[223] or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the ECC scheme; (iv) specific evaluation criteria and methods used in order to demonstrate that the above-mentioned security objectives are achieved; (v) rules for monitoring compliance with the requirements of the certificates or the EU statement of conformity including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements; (vi) rules concerning the consequences of non-conformity of certified ICT products, services and processes; (vii) rules concerning how previously undetected cybersecurity vulnerabilities are to be reported and dealt with; (viii) identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, services or processes; (ix) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued including the period **6-041**

[221] Cybersecurity Act art.54.3.

[222] Cybersecurity Act art.51.

[223] Regulation (EU) No.1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No.1673/2006/EC of the European Parliament and of the Council [2012] OJ L316/12.

of the storage of the EU statement of conformity and the technical documentation of all relevant information by the manufacturer or provider; (x) the maximum period of validity of certificates; (xi) the disclosure policy for granted, amended and withdrawn certificates as well as the conditions for the mutual recognition of certification schemes with third countries. Where applicable, the adopted ECC schemes should also detail: (i) specific or additional requirements applicable to conformity assessment bodies in order to guarantee their technical competence to evaluate the cybersecurity requirements; (ii) information to be supplied or otherwise be made available to the conformity assessment bodies by an applicant which is necessary for certification; (iii) conditions for granting and renewing a certificate, as well as maintaining, continuing, extending or reducing the scope of certification and, finally, rules concerning the retention of records by conformity assessment bodies. Moreover, where the scheme provides for marks or labels, the conditions under which such marks or labels may be used should also be detailed.[224]

6-042 **Assurance levels** In addition, depending on the identified level of risk in terms of the probability and impact of an incident as well as on the rigour and depth of the evaluation methodology, an ECC scheme may specify one or more of the following assurance levels: basic, substantial and/or high.[225] These assurance levels refer to a certificate or an EU statement of conformity issued in the context of a ECC scheme, which provides for each assurance level's respective security requirements, including security functionalities and the corresponding degree of effort for the evaluation of an ICT process, product or service. The certificate or the EU statement of conformity is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.

6-043 **Conformity self-assessment** Only for ICT products, services and processes of low risk corresponding to assurance level basic, an ECC scheme may allow for carrying out a conformity assessment under the sole responsibility of the manufacturer or provider.[226] By drawing up an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated, the manufacturer or provider assumes responsibility for the compliance with the requirements set out in the scheme and must keep all relevant information relating to the conformity at the disposal of the national cybersecurity certification authority for the period provided for in the corresponding ECC scheme.[227] A copy of the EU statement of conformity must be submitted to the national cybersecurity certification authority and to ENISA.[228] EU statements of conformity are recognised in all Member States and are voluntary unless otherwise specified in the Union law or in Member States law.[229]

6-044 **Cybersecurity certification** For assurance level "basic" or "substantial", a European cybersecurity certificate may be issued by conformity assessment bodies on the basis of criteria included in the ECC scheme.[230] Conformity assessment bodies meeting the requirements set out in the Annex of the Cybersecurity Act must be accredited by the national accreditation body named pursuant to Regulation (EC) No.765/2008.[231] Where applicable, the conformity assessment bodies shall be authorised by the national cybersecurity certification authority to carry out its tasks when they meet specific or additional requirements set out in the ECC scheme.[232] Accreditations are issued for a maximum of five years and may be renewed on the same conditions, provided that the conformity assessment body meets the aforementioned requirements.[233] By way of derogation, in duly justified cases, a particular ECC scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body, which may be a national cybersecurity certification authority or a public body that is accredited as a conformity assessment body.[234] In cases where an ECC scheme requires an assurance level "high", the certificate can only be issued by a national cybersecurity certification authority or by an accredited conformity assessment body upon prior approval by the national cybersecurity certification authority for each individual certificate issued or upon prior general delegation of this task by the national cybersecurity certification authority.[235] ICT products, services and processes that have been certified under an ECC scheme shall be presumed to comply with the requirements of such scheme.[236] A European cybersecurity certificate is recognised in all Member States and is voluntary, unless otherwise specified by Union law or Member State law.[237] Indeed, the Commission must regularly assess the efficiency and use of the adopted ECC schemes and whether a specific scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity in the Union and improve the functioning of the internal market.[238] Based on the outcome of those assessments, the Commission shall identify the ICT products, services and processes covered by an existing certification scheme, which are to be covered by a mandatory certification scheme. As a priority, the Commission shall focus on the OES sectors listed in Annex II of the NIS Directive.[239] The natural or legal person who submits ICT products, services or processes for certification shall make available to the national cybersecurity certification authority, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body, all information necessary to conduct the certification.[240] The holder of a certificate must also inform the authority or body issuing the certificate about any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, service or process that may have an impact on its compliance with the requirements related to the certification. That authority or body shall

[224] Cybersecurity Act art.54.
[225] Cybersecurity Act art.52.
[226] Cybersecurity Act art.53.1.
[227] Cybersecurity Act art.53.2.
[228] Cybersecurity Act art.53.3.
[229] Cybersecurity Act art.53.4.

[230] Cybersecurity Act art.56.4.
[231] Regulation (EC) No.765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No.339/93 [2008] OJ L218/30.
[232] Cybersecurity Act art.60.3.
[233] Cybersecurity Act art.60.4.
[234] Cybersecurity Act art.56.5.
[235] Cybersecurity Act art.56.6.
[236] Cybersecurity Act art.56.1.
[237] Cybersecurity Act art.56.2.
[238] The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter.
[239] Cybersecurity Act art.56.3.
[240] Cybersecurity Act art.56.7.

forward that information without undue delay to the national cybersecurity certification authority concerned.[241] Certificates may be issued for the period defined by the particular certification scheme and may be renewed, provided that the relevant requirements continue to be met.[242]

6-045 **Cybersecurity information to be provided by manufacturers or providers** European cybersecurity certificates and EU statements of conformity should help end users to make informed choices. Therefore, the manufacturer or provider of certified ICT products, services or processes for which an EU statement of conformity has been issued must make publicly available supplementary cybersecurity information. This information must include guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services; the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates; contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers; a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, service or process and to any relevant cybersecurity advisories.[243] This information must be available in electronic form and be updated as necessary at least until the expiry of the corresponding European cybersecurity certificate or EU statement of conformity.[244]

6-046 **Website on European cybersecurity certification schemes** ENISA must maintain a dedicated website providing information on, and publicising, ECC schemes, European cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information that the manufacturers or providers of certified ICT products, services or processes or for which an EU statement of conformity has been issued must make publicly available. Where applicable, the website shall also indicate the national cybersecurity certification schemes that have been replaced by a ECC scheme.[245]

6-047 **National cybersecurity certification authorities** Each Member State must designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State.[246] Each national cybersecurity certification authority must be independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making.[247] Moreover, Member States must ensure that the activities of the national cybersecurity certification authorities that relate to the issuance of European

[241] Cybersecurity Act art.56.8.
[242] Cybersecurity Act art.56.9.
[243] Cybersecurity Act art.55.1.
[244] Cybersecurity Act art.55.2.
[245] Cybersecurity Act art.50.
[246] Cybersecurity Act art.58.1.
[247] Cybersecurity Act art.58.3.

cybersecurity certificates are strictly separated from their supervisory activities and that those activities are carried out independently from each other.[248] Amongst other tasks, national cybersecurity certification authorities must supervise and enforce rules included in ECC schemes for the monitoring of the compliance of ICT products, services and processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories; monitor compliance with and enforce the obligations of the manufacturers or providers that are established in their respective territories; actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies; handle complaints by natural or legal persons, investigate the subject matter of such complaints to the extent appropriate and inform the complainant of the progress and the outcome of the investigation within a reasonable period.[249]

6-048 **Right to lodge a complaint and right to a judicial remedy** Natural and legal persons have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body, with the relevant national cybersecurity certification authority. The authority or body with which the complaint has been lodged must inform the complainant of the progress of the proceedings, of the decision taken, and of the right to an effective judicial remedy.[250] Furthermore, notwithstanding any administrative or other non-judicial remedies, natural and legal persons have the right to an effective judicial remedy with regard to decisions taken by the abovementioned authority or body including, where applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons as well as with regard to a failure to act on a complaint lodged with the authority or body. Such proceedings must be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.[251]

6-049 **Penalties** Member States must lay down the rules on penalties applicable to infringements of Title III of the Cybersecurity Act and to infringements of ECC schemes, and take all measures necessary to ensure that they are implemented. These penalties must be effective, proportionate and dissuasive.[252]

[248] Cybersecurity Act art.58.4.
[249] Cybersecurity Act art.58.7.
[250] Cybersecurity Act art.63.
[251] Cybersecurity Act art.64.
[252] Cybersecurity Act art.65.