Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 18 May 2021

WK 6380/2021 COR 1

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI
PROCIV

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
N° Cion doc.:	14150/20 [COM (2020) 823 final]
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148: interaction with sectoral legislation - Comments by IE delegation

Delegations will find in Annex comments by IE delegation on the above-mentioned subject. Comments by CZ were wrongly attributed to IE in WK 6380/2021 INIT.

IRELAND

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

(Text with EEA relevance)

(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission should issue guidelines to Member States in relation to their proposed implementation of the *lex specialis*. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

(13) Regulation XXXX/XXXX of the European Parliament and of the Council[1] should be considered to be a sector-specific Union legal act in relation to this Directive with regard to the financial sector entities. The provisions of Regulation XXXX/XXXX relating to information and communications technology (ICT) risk management measures, management of ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk should apply instead of those set up under this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows the European Supervisory Authorities (ESAs) for the financial sector under Regulation XXXX/XXXX, to participate in thetechnical workings of the Cooperation Group, and to exchange information and cooperate on supervisory aspects under this Directive and with the national CSIRTs. The competent authorities and where relevant the financial entities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents also to the single points of contact or directly to CSIRTs designated under this Directive. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.

[1] *[insert the full title and OJ publication reference when known]*

(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[2] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information exchange on identity of entities within scope of both Directives, information sharing on national strategies, national risk assessments, incidents and cyber threats and the exercise of supervisory and enforcement tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, the initial notifications of cyber threats, near misses and incidents affecting critical entities as well as on the results of supervisory tasks. In particular circumstances competent authorities under Directive (EU) XXX/XXX may request competent authorities under this Directive to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.

(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way so as to facilitate, where appropriate, a timely operational response. The single points of contact should be tasked with forwarding incident notifications to the single points of contact of other affected Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts may also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive. Where appropriate, CSIRTs should also be enabled to receive reports directly from financial entities under the DORA Regulation.

(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[3] and Directive (EU) 2018/1972 of the European Parliament and of the Council[4] related to the imposition of security and notification requirement on these types of entities should therefore be repealed.

---

2 *[insert the full title and OJ publication reference when known]*

3 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 (OJ L 257, 28.8.2014, p. 73).

4 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

(49) Where appropriate and to avoid unnecessary disruption, existing national guidelines and national legislation adopted for the transposition of the rules related to security measures laid down in Article 40(1) of Directive (EU) 2018/1972, as well as of the requirements of Article 40(2) of that Directive concerning the parameters related to the significance of an incident, should continue to be used until transposition arrangements implemented by the Member States. Guidance documentation from ENISA on security and reporting arrangements for entities that are subject to obligations from Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 that are to be replaced by provisions in this Directive would facilitate harmonisation, transition and minimise disruption.

(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should where appropriate cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC.

(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in accordance with the competition rules of the Union as well as the data protection Union law rules.

(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned or in the case of public authorities performance of a task in the public interest, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of various types of personal data

Article 2

Scope

1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.[6]

[6] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:

(a) the services are provided by one of the following entities:

(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;

(ii) trust service providers referred to point 8 of Annex I;

(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;

(b) the entity is a public administration entity as defined in point 23 of Article 4;

(c) the entity is the sole provider of a service in a Member State;

(d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;

(e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;

(f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;

(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[7] [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive and the relevant competent authorities under this Directive are informed of such identifications in accordance with Article 5(4) of the CER Directive.

Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.

3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.

4. This Directive applies without prejudice to Council Directive 2008/114/EC[8] and Directives 2011/93/EU[9] and 2013/40/EU[10] of the European Parliament and of the Council.

---

7 *[insert the full title and OJ publication reference when known]*

8 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

9 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

10 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive**,** such as information exchange among financial authorities referred to in Article 41 of the DORA Regulation or resilient authorities referred to under Article 8 of the CER Directive and competent authorities designated in accordance with Article 8 of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.

6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.

Article 4

Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'network and information system' means:

(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;

(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) 'security of network and information systems' means the ability of network and information systems, of electronics comunications services and of trust services 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 of the related services offered by, or accessible via, those network and information systems, those electronic communications services and those trust services;

(2a) 'electronic communications services' means electronics communications services within the meaning of Article 2(4) of Directive (EU) 2018/1972;

(2b) 'trust services' means trust services within the meaning of Article 3(16) of Regulation (EU) No 910/2014;

(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[11];

[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

(4) ‘national strategy on cybersecurity’ means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;

(5) ‘incident’ means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems, electronic communications services or trust services;

(6) ‘incident handling’ means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;

(7) ‘cyber threat’ means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881;

(8) ‘vulnerability’ means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a cyber threat;

(9) ‘representative’ means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;

(10) ‘standard’ means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[12];

(11) ‘technical specification’ means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012;

(12) ‘internet exchange point (IXP)’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(13) ‘domain name system (DNS)’ means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;

(14) ‘DNS service provider’ means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;

(15) ‘top–level domain name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration

---

cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p.15).

12 Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316,14.11.2012,p.12).

of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers;

(16) 'digital service' means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council [13];

(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[14];

(18) 'online search engine' means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[15];

(19) 'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources;

(20) 'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

(21) 'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);

(23) 'public administration entity' means an entity in a Member State that complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality;

(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law;

---

13 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L. 241, 17.9.2015, p.1).

14 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

15 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.

(24) 'entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

(25) 'essential entity' means any entity of a type referred to as an essential entity in Annex I;

(26) 'important entity' means any entity of a type referred to as an important entity in Annex II.

Article 5

National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall as a minimum address all of the sectors in Annex 1 and 2 and the scope of the financial sector under the Digital Operational Resilience Act Regulation.. The national cybersecurity strategy shall include, in particular, the following:

   (a) a definition of objectives and priorities of the Member States' strategy on cybersecurity;

   (b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors;

   (c) an assessment to identify relevant assets and cybersecurity risks in that Member State;

   (d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;

   (e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;

   (f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[16] [Resilience of Critical Entities Directive] for the purposes of i information exchange on identity of entities within scope of both Directives, nformation sharing on national strategies, national risk assessments, incidents and cyber threats and the exercise of supervisory and enforcement tasks.

2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:

[16] *[insert the full title and OJ publication reference when known]*

(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;

(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;

(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;

(d) a policy related to sustaining the general availability and integrity of the public core of the open internet;

(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;

(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;

(g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;

(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.

3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is strictly necessary to preserve national security.

4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.

Article 11

Cooperation at national level

1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.

2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20.

3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant to this Directive.

4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall facilitate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[17] [the DORA Regulation] within that Member State.

5. Member States shall ensure that their competent authorities regularly provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] onnear misses,, cyber threats,incidents and on the results of supervisory tasks affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those near misses, cyber threats, incidents and on the results of supervisory tasks.

Article 12
Cooperation Group

1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Directive, a Cooperation Group is established.

2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.

3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17 and 42 of Regulation (EU) XXXX/XXXX [the DORA Regulation] shall participate in relevantactivities of the Cooperation Group and exchange information on draft regulatory technical standards being developed under the DORA Regulation..

   Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.

   The Commission shall provide the secretariat.

4. The Cooperation Group shall have the following tasks:

   (a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;

   (b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, building capacity as well as standards and technical specifications;

[17] *[insert the full title and OJ publication reference when known]*

(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;

(d) exchanging advice and cooperating with the Commission on draft Commission implementing or delegated acts adopted pursuant to this Directive;

(e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;

(f) discussing reports on the peer review referred to in Article 16(7);

(g) discussing results from joint-supervisory activities in cross-border cases as referred to in Article 34;

(h) providing strategic guidance to the CSIRTs network on specific emerging issues;

(i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs;

(j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges;

(k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA.

5. The Cooperation Group may request from the CSIRT network a technical report on selected topics.

6. By … [24 months after the date of entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.

7. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

8. The Cooperation Group shall meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to undertake strategic cooperation and facilitate exchange of information. This should include an overview of the state of resilience and of the state of cybersecurity at EU level for each of the sectors set out in Annex 1 to both Directives.

Article 20

Reporting obligations

1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs

3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.

Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.

3. An incident shall be considered significant if:

(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned;

(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.

4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:

(a) without undue delay and in any event within 24 hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

(b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;

(c) a final report not later than one month after the submission of the report under point (a), including at least the following:

(i) a detailed description of the incident, its severity and impact;

(ii) the type of threat or root cause that likely triggered the incident;

(iii) applied and ongoing mitigation measures.

Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) and (c).

4a Member States may require use of one single entry point for receipt of all notifications under this Directive, under Regulation (EU) 2016/679 and Directive 2002/58/EC. Where such a single entry point is being deployed, the enabling facility must have sufficient resilience and security.

5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of

the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1 , the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.

6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.

8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.

9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

10. Competent authorities shall facilitate the prompt provision to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on the initial notifications received in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] in circumstances where the operations of that entity have been disrupted.

11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Article 21

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to usecertain ICT products, ICT services and ICT processes certified under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 or under recognised international standards. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

.

Article 26

Cybersecurity information-sharing arrangements

1. Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves and optionally with CSIRTs and competent authorities including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:

   (a) aims at preventing, detecting, responding to or mitigating incidents;

   (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.

   The exchange of such information may include personal data in which case it is in accordance with the relevant provisions on lawfulness of processing under Article 6(1) of Regulation (EU) 2016/679, namely for the purposes of legitimate interests, or in the case of public authorities such as CSIRTs and competent authorities performance of a task in the public interest.

2. Member States shall ensure that the exchange of information takes place within trusted communities of essential and important entities and where appropriate CSIRTs and competent authorities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared and in accordance with the rules of Union law referred to in paragraph 1.

3. Member States shall set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).

4. Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2,

upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.

Article 29

Supervision and enforcement for essential entities

1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:

   (a) on-site inspections and off-site supervision, including random checks;

   (b) regular audits;

   (c) targeted security audits based on risk assessments or risk-related available information;

   (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;

   (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);

   (f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;

   (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:

   (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;

   (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;

   (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;

(d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;

(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;

(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;

(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:

(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;

(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.

These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.

7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:

   (a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.

   (b) the duration of the infringement, including the element of repeated infringements;

   (c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;

   (d) the intentional or negligent character of the infringement;

   (e) measures taken by the entity to prevent or mitigate the damage and/or losses;

   (f) adherence to approved codes of conduct or approved certification mechanisms;

   (g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.

8. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.

9. Member States shall ensure that their competent authorities inform the relevant competent authorities of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. In particular circumstances competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]may request competent authorities toexercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

10. Competent authorities designated under Article 8 that have supervisory and enforcement tasks for the digital infrastructure sector may inform national financial authorities designated under the DORA Regulation when exercising their supervisory and enforcement powers aimed at ensuring compliance with the obligations pursuant to this Directive. Upon request of such national financial authorities or the lead overseer under the DORA Regulation, these competent authorities may exercise their supervisory and enforcement powers on an essential entity in the digital infrastructure

sector that is designated as a critical ICT third-party service provider under the DORA Regulation.

1. .

Article 39

Amendment of Regulation (EU) No 910/2014

Article 19 of Regulation (EU) No 910/2014 is deleted with effect from [the day following the date of transposition deadline of the Directive].

With a view towards ensuring a smooth transition, ENISA shall publish guidance on the applicability of cybersecurity risk management measures in Article 18 and of interpretation of significance of an incident in Article 20 for providers of trust services within 6 months of the Directive entering into force. Such guidance shall cease on adoption of implementing acts by the Commisson in accordance with the provisions in Article 18(5) and Article 20(11).

Article 40

Amendment of Directive (EU) 2018/1972

Articles 40 and 41 of Directive (EU) 2018/1972 are deleted with effect from [the day following the date of transposition deadline of the Directive.

With a view towards ensuring a smooth transition, ENISA shall publish guidance on the applicability of cybersecurity risk management measures in Article 18 and of interpretation of significance of an incident in Article 20 for providers of public electronic communication networks and providers of publicly available electronic communications services within 6 months of the Directive entering into force. Such guidance shall cease on adoption of implementing acts by the Commisson in accordance with the provisions in Article 18(5) and Article 20(11)