Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359 (COD)

Brussels, 01 July 2021

WK 8685/2021 ADD 1

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI
CODEC

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

NOTE

From: To:	General Secretariat of the Council Delegations
N° prev. doc.: N° Cion doc.:	WK 8155/21 ST 14150 2020 INIT
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 2016/1148 - Interaction of NIS 2 with sectoral legislation: Comments by AT, EE, PL delegations

Delegations will find in Annex comments by AT, EE, PL delegations on the above mentioned subject

Table of Contents

AUSTRIA

Recitals

(12) **This Directive sets out the baseline for cybersecurity risk management measures and reporting obligations across all sectors that fall within its scope. ~~This Directive also provides an empowerment for implementing and delegated acts that may further specify the elements of the cybersecurity risk management measures or the reporting obligations, including in relation to sectorial specificities for sectors within the scope of this Directive.~~ In order to avoid unnecessary fragmentation of cybersecurity provisions of Union legal acts, when additional sector-specific provisions pertaining to cybersecurity risk management measures and ~~notification~~ reporting obligations appear to be necessary to ensure high levels of cybersecurity, an assessment should be ~~considered~~ made by the Commission as to whether such provisions ~~can~~ could be stipulated in an implementing or delegated act ~~in relation to which empowerment is provided for in this Directive.~~. Should such ~~implementing or delegated~~ acts not be suitable for this purpose,** sector-specific legislation and instruments **could~~an~~** contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. **At the same time, such sector-specific provisions of Union legal acts should duly take account of the need for a comprehensive and consistent cybersecurity framework.** ~~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.

(12a) Where a sector–specific Union legal act requires essential or important entities to adopt **measures of at least an equivalent effect to the obligations laid down in this Directive~~, and in particular~~ related to** cybersecurity risk management measures **and obligations** to notify **significant** 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. **Where the respective Union legal act containing such sector-specific provisions lays down corresponding rules on supervision and enforcement, the latter should also apply. When determining the equivalent effect of the obligations set out in the sector-specific provisions of an Union legal act, the following aspects should be considered: (i) the cybersecurity risk management measures should consist of appropriate and proportionate governance requirements and technical and organizational measures to manage the risks posed to the security of network and information systems which the relevant entities use in the provision of their services and should include as a minimum all the elements laid down in this Directive; (ii) the requirement to notify significant incidents and cyber threats should (be at least equivalent with/reflect at the minimum) the obligations set out in this Directive as regards the content, format and timelines of the notifications; (iii) the ~~requirements concerning the interaction between the~~ reporting modalities by entities ~~and the relevant authorities~~of sector-specific Union legal acts should (be at least**

equivalent with/reflect at the minimum) the requirements set out in this Directive as regards their content, format and timelines and should take into account the role of CSIRTs; (iv) the cross-border cooperation requirements for the relevant authorities should (be at least equivalent with/reflect at the minimum) those set out by this Directive. If the sector-specific provisions of a Union legal act do not cover all entities in a specific sector falling within the scope of this Directive, the provisions of this Directive should continue to apply to the entities not covered by those sector-specific provisions. The Commission **should regularly assess the application of the equivalent effect requirement in relation to sector-specific provisions of Union legal acts and** may issue guidelines**, recommendations on necessary actions or measures to be taken by the competent authorities designated under sector-specific Union legal acts in order to address possible gaps with provisions under this ~~regard~~Directive.** ~~relation to the implementation of the *lex specialis*.~~ **The Commission ~~should~~shall consult the Cooperation Group when preparing the regular assessment and developing the potential guidelines.**

(12ab) Key definitions outlined in Article 4 of this Directive should serve as a baseline for sector-specific Union legal acts.

(12aa) When sector-specific provisions of Union legal acts require essential or important entities to adopt measures of at least an equivalent effect to the ~~notification~~reporting obligations laid down in this Directive, overlapping of reporting obligations should be avoided, and coherence and effectiveness of handling of notifications of cyber threats or incidents should be ensured. For this purpose, the above-mentioned sector-specific provisions may ~~provide for~~allow Member States to establish a common, automatic and direct reporting mechanism for significant incidents and cyber threats to both the authorities whose tasks are set out in the respective sector-specific provisions and the competent authorities, including the single point of contact and CSIRTs as appropriate, responsible for the cybersecurity tasks provided for in this Directive or for ~~an automatic and direct~~ a mechanism that ensures ~~timely~~systematic and immediate sharing of information and cooperation among the relevant authorities and CSIRTs concerning the handling of such notifications. For the purposes of simplifying reporting and for implementing the common, automatic and direct reporting mechanism, Member States may utilise the single-entry point they establish according to Article 11(5a) of this Directive. To ensure harmonisation, reporting obligations of sector-specific Union legal acts should be aligned with those specified under this Directive.

(13) Regulation XXXX/XXXX of the European Parliament and of the Council 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, ~~information sharing~~ and reporting obligations, 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 ~~all financial supervisors,~~ the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX, to participate in **the** ~~strategic policy discussions and technical~~ workings of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive and with the national CSIRTs. The competent authorities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents **and significant cyber threats** also to the single points of contact **or the national CSIRTs** designated under this Directive. **This can be achieved, for example, by automatic and direct forwarding of incident notifications or a common reporting platform.** 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.

(13a) In order to avoid gaps and duplications of cybersecurity obligations imposed on entities in the aviation sector referred to in Annex I (2) (a), competent authorities under Commission Implementing Regulation 2019/1583 and competent authorities under this Directive should cooperate in relation to the implementation of cybersecurity risk management measures and the supervision of those measures at national level. The compliance of an entity with the cybersecurity risk management measures under this Directive may be considered by the competent authorities under Commission Implementing Regulation 2019/1583 as compliance with the requirements laid down in that Regulation.

(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 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 sharing on incidents, and cyber threats, and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents **as well as on non-cyber risks, threats and incidents** affecting critical entities or **entities equivalent to critical entities** ~~as well as on~~ **including** the cybersecurity **and physical** measures taken by critical entities **and the results of supervisory measures carried out with regard to such entities**. **Furthermore, in order to streamline supervisory activities between the competent authorities designated under both directives and in order to minimize the administrative burden for the entities, competent authorities should endeavour to align incident notification templates and supervisory processes.** ~~Upon request of~~ **Where appropriate**, competent authorities under Directive (EU) XXX/XXX, **may request** competent authorities under this Directive ~~should be allowed~~ to exercise their supervisory and enforcement powers on an essential entity identified as critical. ~~**The** Both authorities~~**Aauthorities under both Directives** should cooperate and exchange information for this purpose.

(14a) Union law on the protection of personal data and privacy applies to any processing of personal data falling within the scope of this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council and therefore should not affect notably the tasks and powers of the independent supervisory authorities competent to monitor compliance with the respective Union data protection law.

(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council18, as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services, while taking into due account the degree of their dependence on network and information systems. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.

(23) **Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way also with a view to facilitate, where appropriate, a timely ~~operational response~~ response to incidents in accordance with Article 10(2c) and to provide a response to the notifying entity in accordance with Article 20(5).** 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 should also be the addressees of relevant information on **major ICT** incidents **and significant cyber threats** concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX. ~~**Member States may additionally determine that: (a) the competent authority should immediately and automatically in a timely manner provide the initial notification and each report referred to in Article 17 paragraph 3 [of Regulation XXX DORA] to the national single point of contact, the national competent authorities or the national Computer Security Incident Response Teams designated, respectively, in accordance with this Directive; (b) some or all financial entities should also provide the initial notification and each report referred to Article 17, paragraph 3 [of Regulation XXX DORA] using the template referred to in Article 18 [of Regulation XXX DORA] to the national competent authorities or the national Computer Security Incident Response Teams designated in accordance with this Directive.~~ **For this purpose, Member States may determine that competent authorities or national CSIRTs are adressees of the notifications in accordance with Regulation EU [of Regulation XXX DORA].** ~~which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.~~

(23a) **Competent authorities of sector specific lex specialis may exercise the supervision and enforcement over obligations given in those sector specific lex specialis with the assistance of the competent authority designated in accordance with this Directive. In order to achieve this, the competent authorities concerned should establish effective cooperation arrangements. Such cooperation arrangements shall specify amongst others, the procedures concerning the coordination of supervisory activities, including the procedures of investigations and on-site inspections in accordance with the national law and mechanism for the exchange of information between competent authorities, including access to information requested by competent authority designated in accordance with this Directive.**

(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive. CSIRTs should be able to exchange information, including personal data, with national CERTs and CSIRTs of third countries for the purpose of their tasks. Such disclosure or exchange may constitute important reasons of public interest, especially in the event of a significant incident or cyber threat having significant effect on the provision of service.

(40a) As threats to the security of network and information systems can have different origins, this Directive applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment from any event such as theft, fire, flood, telecommunications ~~or power failures~~, power failures or from any unauthorized physical access and damage to and interference with the organisation's information and information processing facilities that could compromise 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. The risk- management measures should therefore ~~in particular~~also address the physical and environmental security by including measures to protect the entity's network and information systems from system failures, human error, malicious actions or natural phenomena in line with internationally recognised standards, such as included in ISO 27000 series. Those measures should be in line with Directive XXXX [CER Directive].

~~(42a) In order to demonstrate compliance with cybersecurity risk management measures, Member States may require essential and important entities to use trust services or notified electronic identification schemes under Regulation 910/2014. Member States may also require entities to use particular ICT products, services and processes certified under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The ICT products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.~~

(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 and Directive (EU) 2018/1972 of the European Parliament and of the Council related to the imposition of security and notification requirement on these types of entities should therefore be repealed and appropriately complemented in this Directive. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council.**

(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)~~ and 41 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 by the competent authorities in charge of supervision and enforcement for the purposes of this Directive~~ **be taken into account in transposition arrangements implemented by the Member States in relation to this Directive, thereby building on the knowledge and skills already acquired under Directive (EU) 2018/1972 concerning security risk management measures and incident notifications. ENISA may also develop guidance documentation on security and reporting arrangements for entities that were subject to obligations from Directive (EU) 2018/1972 to facilitate harmonisation, transition and minimise disruption ~~continue to be used by the competent authorities in charge of supervision and enforcement for the purposes of this Directive~~. Member States may assign the role of competent authorities for electronic communications to the national regulatory authorities in order to ensure the continuation of current practices and to build on the knowledge and experience gained in Directive (EU) 2018/1972.**

(69) ~~The processing of personal data, t~~**T**o the extent strictly necessary and proportionate for the purposes of ensuring network and information security**, the processing of personal data** by **essential and important** entities, ~~public authorities, CERTs, CSIRTs,~~ and providers of security technologies and services **or the processing of personal data within the Cooperation Group, CSIRT network and CyCLONe and cybersecurity information sharing arrangements established under this Directive** should constitute a legitimate interest of the data controller concerned, ~~as referred to in Regulation (EU) 2016/679~~ **and processing of personal data by competent authorities, SPOCs and CSIRTs ~~should be laid down in~~or the processing of personal data within the Cooperation Group, CSIRT network and CyCLONe established under this Directive should be laid down in Union or national law and considered necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest or the exercise of official authority vested in the data controller, as referred to in Article 6(1)(c) or (e) of 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 ~~the following~~ **various** types of personal data**, such as:** IP addresses, uniform resources locators (URLs)**,** domain names, and email addresses. **The transfer of personal data by CSIRTs to a third country or an international organisation, may be necessary for important reasons of public interest, to the extent that this is strictly necessary and proportionate for the purposes of ensuring network and information security by essential or important entities, as referred to in Annex I and II, especially in case of a incidents and cyber threat having a significant impact on the provision of services, in the light of the objectives of this Directive and in particular the tasks of CSIRTs for the aforementioned entities.**

(80) ~~In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making26 . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.~~

Articles

Article 2
Scope

(...)

~~3. This Directive is without prejudice to the **responsibility** competences of Member States concerning the maintenance of ***regarding essential State functions*** ***concerning*** public security, defence and national security ***in accordance*** in compliance with Union law.")~~

3.a This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.

(...)

5a. To the extent that is strictly necessary and proportionate for the purposes of ensuring the security of network and information systems of essential and important entities, competent authorities, SPOCs and CSIRTs may process special categories of personal data referred to in Article 9 (1) of Regulation (EU) 2016/679 subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

6. Where provisions of sector–specific **Union legal** acts ~~of Union law~~ require essential or important entities ~~either~~ to adopt cybersecurity risk management measures or to notify **significant** 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 provisions on supervision and enforcement laid down in Chapter VI~~, shall not apply **to those entities**. **Where the respective Union legal act containing such sector-specific provisions lays down corresponding rules on supervision and enforcement, Chapter VI should not apply to those entities either.**

7. In order to safeguard a coherent minimum standard of cybersecurity across all sectors, sector-specific Union legal acts referred to in paragraph 6 should include:

(a) cybersecurity risk management measures, that are at a minimum equivalent to those laid down in article 18 paragraphs 1 and 2 of this Directive; and

(b) requirements to notify significant incidents or cyber threats that are, at a minimum, equivalent to those laid down in article 20 paragraphs 1 through 4 and further include:

(i) where appropriate, automatic and direct access to the incident notifications by the national competent authority under this Directive through a common reporting mechanism; or

(ii) where appropriate, automatic and direct forwarding of the notifications to the national competent authority under this Directive or the national Computer Security Incident Response Teams designated in accordance with this Dircetive by the authority that receives incident notifications under the sector-specific Union legal act.

(c) requirements concerning cross-border cooperation for the relevant authorities shall be at least equivalent with those set out by this Directive.

8. The Commission shall periodically review the application of the equivalent effect requirement in paragraph 6 and 7 in relation to sector-specific provisions of Union legal acts. The Commission shall consult the Cooperation Group and relevant expert groups established by the sector-specific Union legal acts when preparing these regular assessments and developing the potential guidelines, recommendations on necessary actions or measures.

9. When additional sector-specific provisions pertaining to cybersecurity risk management measures and notification obligations appear to be necessary to ensure high levels of cybersecurity, the Commission should assess whether such provisions can be stipulated in an implementing or delegated act referred to in Article 18 (5) and (6) of this Directive.

Article 4
Definitions

(...)

~~(2)~~ 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any ~~action~~ **event** that **may** compromise**~~s~~** 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;

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

(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;

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

(16b) 'Qualified trust service provider' means a qualified service provider within the meaning of article 3(20) of Regulation 910/2014;

(…)

Article 5
National cybersecurity strategy

(…)

1.(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 [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents**~~, and~~** cyber threats **and other non-cyber incidents and threats ~~and~~ as well as** the exercise of supervisory tasks**, as appropriate.**

(…)

Article 10
Requirements and Tasks of CSIRTS
(…)

3a. CSIRTs shall establish cooperation relationships with national CERTs and CSIRTs of third countries and may exchange relevant, necessary and proportionate information in view of their tasks, which, in this context, can create an important reason of public interest

Article 11
Cooperation at national level

(...)

4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the **competent** authorities **designated** ~~responsible for critical infrastructure~~ pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive~~]~~**], the competent authorities under Commission Implementing Regulation 2019/1583, national regulatory authorities designated in accordance with Directive (EU) 2018/1972, the national authorities designated pursuant to Article 17 of Regulation (EU) No 910/2014,** ~~and~~ the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation~~]~~**], as well as competent authorities designated by other sector-specific Union legal acts** within that Member State.

5. Member States shall ensure that their competent authorities **under this Directive and the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]** regularly **exchange** ~~provide~~ information ~~to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]~~ on **the identification of critical entities,** cybersecurity risks, cyber **threats and incidents as well as on non-cyber risks, threats and incidents** 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 risks and incidents.

5.a For the purposes of simplifying the reporting of ~~security~~ incidents ~~which entail a possible personal data breach~~, Member States ~~shall~~may establish a single-entry point for all notifications required under this Directive, as well as under Regulation (EU) 2016/679 and Directive 2002/58/EC, where appropriate, when such incidentes entail a possible personal data breach. Member States may integrate notifications required under other sector-specific Union legal acts in the single-entry-point. This single-entry point shall not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to independent ~~suprvisory~~supervisory authorities.

5b. Member States shall ensure that their competent authorities under this Directive and the competent authorities designated pursuant to Regulation (EU) XXXX/XXXX [DORA Regulation] regularly exchange information on cybersecurity risks, cyber threats and incidents affecting essential entities who may be financial entities or critical third party ICT service providers, pursuant to Regulation (EU) XXXX/XXXX [DORA Regulation], as well as the measures taken by competent authorities in response to those risks and incidents.

5c Information covered by professional secrecy may not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law, including the exchange of information among competent authorities designated pursuant to Regulation (EU) XXXX/XXXX [DORA Regulation] or competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and competent authorities designated in accordance with Article 8 of this Directive.

5d Member States shall ensure that their competent authorities under this Directive and the supervisory bodies designated pursuant to article 17 of Regulation (EU) No 910/2014 regularly, and at least once per year, exchange information on cybersecurity risks, cyber threats and incidents affecting trust service providers.

Article 12

Cooperation Group

(...)

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(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group. **A meeting with the participation of ESAs shall be held regularly and, at least, once a year.**

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 promote strategic cooperation and **facilitate** exchange of information.

Article 18

Cybersecurity risk management measures

1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network, **services** and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network, services and information systems appropriate to the risk presented.

1a. This Directive applies an "all-hazard" approach that includes the protection of network and information systems and the physical protection from relevant natural and man-made risks that could compromise 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.

(…)

5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications, **as well as sectoral specificities, as necessary,** of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

Article 21

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with ~~certain requirements of Article 18~~ **cybersecurity risk management measures,** Member States may require **all or certain groups of** essential and important entities to ~~certify certain~~ **use trust services or notified electronic identification schemes under Regulation 910/2014. Member States may also require entities to use particular ICT products,** ~~ICT~~ **services and** ~~ICT~~ **processes certified** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. ~~The~~ **in order to demonstrate compliance or establish a presumption of conformity with certain requirements. The ICT** products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

1a . Member States may rely on cybersecurity services providers certified under Regulation (EU) 2019/881 or national certification schemes in the absence of a relevant EU certification scheme to demonstrate compliance with certain requirements of Article 18, or to enforce the supervision activities foreseen in Articles 29 and 30.

2. The Commission shall be empowered to adopt ~~delegated~~ **implementing** acts specifying which categories of essential entities shall be required **to use certain certified ICT products, ~~ICT~~ services and ~~ICT~~ processes or** obtain a certificate ~~and~~ under ~~which~~ specific European cybersecurity certification schemes **adopted pursuant to Article 49 of Regulation (EU) 2019/881**. ~~pursuant to paragraph 1The delegated acts shall be adopted in accordance with Article 36.~~ **When preparing the implementing act, the Commission shall:**

(i) take into account the impact of the measures on the manufacturers or providers of such ICT products, services or processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, services or processes;
(ii) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;
(iii) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, services or processes, particularly SMEs;

3. The Commission may request ENISA to prepare a candidate scheme **or to review an existing European cybersecurity certification scheme** pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.

Article 29

Supervision and enforcement for essential entities

(...)

9. Member States shall ensure that their competent authorities **under this Directive** inform the relevant competent authorities **within that same** ~~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. **Where appropriate**, ~~Upon request of~~ competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]~~,~~ **may request** competent authorities **under this Directive** ~~may~~ **to** exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

10. Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum pursuant to Article 29 (1) of Regulation (EU) XXXX/XXXX [DORA] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity designated as critical ICT third-party service provider pursuant to Article 28 of Regulation (EU) XXXX/XXXX [DORA] with the obligations pursuant to this Directive.

Article 32

Infringements entailing a personal data breach

1. Where the competent authorities have ~~indications~~ **evidence** that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall**, without undue delay,** inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ~~within a reasonable period of time~~.

*Article ~~35~~**36***

~~***Review***~~

Exercise of the delegation

(…)

~~2. **The Commission shall periodically review the application of the equivalent effect requirement in Article 2(6) of this Directive in relation to sector-specific provisions of Union legal acts. The Commission shall consult the Cooperation Group when preparing these regular assessments.**~~**The power to adopt delegated acts referred to in Articles 18(6) ~~and 21(2)~~ shall be conferred on the Commission for a period of five years from […]**

3. The delegation of power referred to in Articles 18(6) **and 21(2)** may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

(…)

Article 38

Transposition

1. Member States shall adopt and publish, by … [~~18~~ **24** months after the date of entry into force of this Directive, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].

(…)

Article 39

Amendment of Regulation (EU) No 910/2014

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

Article 40

Amendment of Directive (EU) 2018/1972

Articles 40 and 41 of Directive (EU) 2018/1972 are deleted **effect from… [date of the transposition deadline of the Directive].**

ANNEXES

With regard to trust service providers, a differentiation of the regulatory treatment between non-qualified and qualified trust service providers could be envisaged with the following proposed amendments in Annex I and II:

i) **In Annex I point 8:- qualified trust service providers referred to in point (19) (20) of Article 3 of Regulation (EU) No 910/2014**

ii) **In Annex II point 6:- non-qualified trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014**

With regard to providers of public electronic communications networks, a precision of the regulatory treatment for micro and small enterprises could be envisaged with the following proposed amendment in Annex I and II:

i) **In Annex I point 8: - Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972(26) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available. This is not applicable to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.**

In Annex II point 6a (new) Digital infrastructure - Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972(26) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available when they qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.

ESTONIA

EE written contribution, NIS 2.0, 29.06.2021

General remarks:

Estonia welcomes the work plan outlined by the Slovenian presidency, but nonetheless hopes that enough time will be dedicated to discuss these central questions to the architecture of the new NIS directive.

NIS2 Reference (doc. No: 9583/1/21)	**Comments**	**Drafting proposal**
Scope of NIS 2.0	We consider the implementation of the size-cap rule as the most optimal and straightforward choice for a common EU solution. Furthermore, we recognise the importance of continuing the identification procedure by the competent authorities. In order to reduce the administrative burden of the competent authorities, entities themselves should notify the authorities. Estonia supports involving the public administration in the scope of the directive, but we see the need of analysing how these measures and requirements would match to the patchwork of different set-ups. As Estonia is considered a single region in both, NUTS I and NUTS II nomenclatures, opting for this classificatory system seems suitable from our viewpoint. Whereas we need more time to analyse the interaction of the new eIDAS and NIS 2.0, we still have a strong reservation towards involving trust service providers in the scope of the NIS 2.0.	
Recital 12a/Recital 12aa/Recital 13/Article 20	Removal of the obligation for entities to report "cyber threats". Notifying cyber threats will bring excessive administrative burden to both, competent authorities and entities.	[…]Where a sector–specific Union legal act requires essential or important entities to adopt **measures of at least an equivalent effect to the obligations laid down in this Directive~~,~~ ~~and in particular~~ <u>related to</u>** cybersecurity risk

		management measures **and obligations** to notify **significant** 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.[…]
Recital 23	We support the new provision related to the possibility of adding CSIRTs or competent authorities as addressees of the notifications of the DORA Regulation.	
Recital 14	Unlike the information that could be exchanged between the competent authorities and entities related to cyber threats, exchange of information between different competent authorities will not bring a substantial administrative burden, but will help all authorities to assess threats and risks better. We thus support the amendments made in this recital.	
Article 2	We support the proposal done by our FR colleagues.	FR: (*New) The entities identified in Annex I and II shall register with the national competent authority by [X months after the transposition deadline]*
Article 10	We welcome the addition of provision related to cooperation between CSIRTs and third countries.	

Article 11	We strongly support the addition of the concept of the single-entry point for all notifications, as it will help to reduce administrative burden, while improving cooperation between different authorities.	
Articles 17-22	We welcome the new approach of having an overarching philosophy for security requirements. However, we deem some of them important in essence, but consider their incorporation in the articles of the Directive as overregulation. For example, Estonia as a small country will quite certainly designate dozens of small enterprises as essential entities, who will not have the resources to assess their supply chains, follow strict encryption policies or use certified products. Moreover, we find it difficult to supervise how much cybersecurity-related training members of managing boards of entities will receive. In the concrete policies that entities have to adopt, we suggest focusing more on cyber hygiene, i.e. policies related to remote working. In regards to reporting obligations, we support the 24-hour deadline of reporting for incidents. We also welcome further debate on formalising the role of CISO in the context of the NIS 2.0.	
Article 39	Amendment of Regulation (EU) No 910/2014	Deletion of the article 39.

POLAND

Polish comments on the Presidency Compromise Proposal of 21 June 2021

on NIS2 Interaction with Sectoral Legislation

Recitals

~~(~~12) **This Directive sets out the baseline for cybersecurity risk management measures and reporting obligations across all sectors that fall within its scope. ~~This Directive also provides an empowerment for implementing and delegated acts that may further specify the elements of the cybersecurity risk management measures or the reporting obligations, including in relation to sectorial specificities for sectors within the scope of this Directive.~~ In order to avoid unnecessary fragmentation of cybersecurity provisions of Union legal acts, when additional sector-specific provisions pertaining to cybersecurity risk management measures and ~~notification~~ reporting obligations appear to be necessary to ensure high levels of cybersecurity, an assessment should be ~~considered~~ made by the Commission as to whether such provisions ~~can~~ could be stipulated in an implementing or delegated act ~~in relation to which empowerment is provided for in this Directive.~~. Should such ~~implementing or delegated~~ acts not be suitable for this purpose,** sector-specific legislation and instruments **could~~an~~** contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. **At the same time, such sector-specific provisions of Union legal acts should duly take account of the need for a comprehensive and consistent cybersecurity framework.** ~~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.

(12a) Where a sector–specific Union legal act requires essential or important entities to adopt **measures of at least an equivalent effect to the obligations laid down in this Directive~~, and in particular~~ related to** cybersecurity risk management measures **and obligations** to notify **significant** 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. **Where the respective Union legal act containing such sector-specific provisions lays down corresponding rules on supervision and enforcement, the latter should also apply.**

When determining the equivalent effect of the obligations set out in the sector-specific provisions of an Union legal act, the following aspects should be considered: (i) the cybersecurity risk management measures should consist of appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which the relevant entities use in the provision of their services and should include as a minimum all the elements laid down in this Directive; (ii) the requirement to notify significant incidents and cyber threats should (be at least equivalent withthe obligations set out in this Directive as regards the content, format and timelines of the notifications; (iii) the ~~requirements concerning the interaction between the~~ reporting modalities by entities ~~and the relevant authorities~~of sector-specific Union legal acts should (be at least equivalent with the requirements set out in this Directive as regards their content, format and timelines and should take into account the role of CSIRTs; (iv) the cross-border cooperation requirements for the relevant authorities should (be at least equivalent withthose set out by this Directive. If the sector-specific provisions of a Union legal act do not cover all entities in a specific sector falling within the scope of this Directive, the provisions of this Directive should continue to apply to the entities not covered by those sector-specific provisions. The Commission **should regularly assess the application of the equivalent effect requirement in relation to sector-specific provisions of Union legal acts and** may issue guidelines or **recommendations on necessary actions or measures to be taken by the competent authorities designated under sector-specific Union legal acts in order to address possible gaps with provisions under this ~~regard~~Directive.** ~~relation to the implementation of the *lex specialis*.~~ **The Commission ~~should~~shall consult the Cooperation Group when preparing the regular assessment and developing the potential guidelines or recommendations.**

12ab)Definitions outlined in Article 4 of this Directive in principle should not be changed by the sector specific legislation. Comprehensive cybersecurity framework requires using a coherent terminology.

(12aa) When sector-specific provisions of Union legal acts require essential or important entities to adopt measures of at least an equivalent effect to the ~~notification~~reporting obligations laid down in this Directive, overlapping of reporting obligations should be avoided, and coherence and effectiveness of handling of notifications of cyber threats or incidents should be ensured.

For this purpose, the above-mentioned sector-specific provisions may ~~provide for~~allow Member States to establish a common, automatic and direct reporting mechanism for significant incidents and cyber threats to both the authorities under sector-specific provisions and the competent authorities, the single point of contact and CSIRTs as appropriate, designated in line with this Directive or ~~an automatic and direct~~ a mechanism that ensures ~~timely~~systematic and immediate sharing of information and cooperation among the relevant authorities and CSIRTs concerning the handling of such notifications. For the purposes of simplifying reporting and for implementing the common, automatic and direct reporting mechanism, Member States may utilise the single-entry point they establish according to Article 11(5a) of this Directive. To ensure harmonisation, reporting obligations of sector-specific Union legal acts should be aligned with those specified under this Directive.

(13) Regulation XXXX/XXXX of the European Parliament and of the Council 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, ~~information sharing~~ and reporting obligations, 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 ~~all financial supervisors,~~ the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX, to participate in **the** ~~strategic policy discussions and technical~~ workings of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive and with the national CSIRTs. The competent authorities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents **and significant cyber threats** also to the single points of contact **or the national CSIRTs** designated under this Directive. **This can be achieved, for example, by automatic and direct forwarding of incident notifications or a common reporting platform.** 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.

(13a) In order to avoid gaps and duplications of cybersecurity obligations imposed on entities in the aviation sector referred to in Annex I (2) (a), competent authorities under Commission Implementing Regulation 2019/1583 and competent authorities under this Directive should cooperate in relation to the implementation of cybersecurity risk management measures and the supervision of those measures at national level. The compliance of an entity with the cybersecurity risk management measures under this Directive may be considered by the competent authorities under Commission Implementing Regulation 2019/1583 as compliance with the requirements laid down in that Regulation.

(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 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 sharing on incidents, and cyber threats, and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, threats, risks and incidents, especially cyber ones affecting critical entities or **entities equivalent to critical entities** ~~as well as on~~ **including** the cybersecurity **and physical** measures taken by critical entities **and the results of supervisory measures carried out with regard to such entities**. **Furthermore, in order to streamline supervisory activities between the competent authorities designated under both directives and in order to minimize the administrative burden for the entities, competent authorities should endeavour to align incident notification templates and supervisory processes.** ~~Upon request of~~ **Where appropriate**, competent authorities under Directive (EU) XXX/XXX, **may request** competent authorities under this Directive ~~should be allowed~~ to exercise their supervisory and enforcement powers on an essential entity identified as critical. ~~The Both authorities~~**Aauthorities under both Directives** should cooperate and exchange information for this purpose.

(14a) Union law on the protection of personal data and privacy applies to any processing of personal data falling within the scope of this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council and therefore should not affect notably the tasks and powers of the independent supervisory authorities competent to monitor compliance with the respective Union data protection law.

(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council18, as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services, while taking into due account the degree of their dependence on network and information systems. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.

(23) **Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way also with a view to facilitate, where appropriate, a timely ~~operational response~~ response to incidents in accordance with Article 10(2c) and to provide a response to the notifying entity in accordance with Article 20(5).** 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 should also be the addressees of relevant information on **major ICT** incidents **and significant cyber threats** concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX. ~~**Member States may additionally determine that: (a) the competent authority should immediately and automatically in a timely manner provide the initial notification and each report referred to in Article 17 paragraph 3 [of Regulation XXX DORA] to the national single point of contact, the national competent authorities or the national Computer Security Incident Response Teams designated, respectively, in accordance with this Directive; (b) some or all financial entities should also provide the initial notification and each report referred to Article 17, paragraph 3 [of Regulation XXX DORA] using the template referred to in Article 18 [of Regulation XXX DORA] to the national competent authorities or the national Computer Security Incident Response Teams designated in accordance with this Directive.~~ **For this purpose, Member States may determine that competent authorities or national CSIRTs are adressees of the notifications in accordance with Regulation EU [of Regulation XXX DORA].** ~~which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.~~

23a) **The sector specific Union legal act may foresee that competent authorities designated under such sector specific act exercise the supervision and enforcement powers with the assistance of the competent authority designated in accordance with this Directive. The competent authorities concerned can conclude cooperation arrangements specifing, in line with national legislation, the practical rules of cooperation.**

(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive. CSIRTs should be able to exchange information, including personal data, with national CERTs and CSIRTs of third countries for the purpose of their tasks. Such disclosure or exchange may constitute important reasons of public interest, especially in the event of a significant incident or cyber threat having significant effect on the provision of service.

(40a) As threats to the security of network and information systems can have different origins, this Directive applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment from any event such as theft, fire, flood, telecommunications ~~or power failures~~, power failures or from any unauthorized physical access and damage to and interference with the organisation's information and information processing facilities that could compromise 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. The risk- management measures should therefore ~~in particular~~also address the physical and environmental security by including measures to protect the entity's network and information systems from system failures, human error, malicious actions or natural phenomena in line with internationally recognised standards, such as included in ISO 27000 series. Those measures should be in line with Directive XXXX [CER Directive].

~~(42a) In order to demonstrate compliance with cybersecurity risk management measures, Member States may require essential and important entities to use trust services or notified electronic identification schemes under Regulation 910/2014. Member States may also require entities to use particular ICT products, services and processes certified under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The ICT products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.~~

(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 and Directive (EU) 2018/1972 of the European Parliament and of the Council related to the imposition of security and notification requirement on these types of entities should therefore be repealed and appropriately complemented in this Directive. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council.**

(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)~~ and 41 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 by the competent authorities in charge of supervision and enforcement for the purposes of this Directive~~ **be duly taken into account by the Member States in the process of transposition of this Directive, thereby building on the knowledge and skills already acquired under Directive (EU) 2018/1972 concerning security risk management measures and incident reporting . ENISA may also develop guidance on security and reporting arrangements for entities that were subject to obligations from Directive (EU) 2018/1972 to facilitate harmonisation, transition and minimise disruption ~~continue to be used by the competent authorities in charge of supervision and enforcement for the purposes of this Directive~~. Member States may assign the role of competent authorities for electronic communications to the national regulatory authorities in order to ensure the continuation of current practices and to build on the knowledge and experience gained in Directive (EU) 2018/1972.**

(69) ~~The processing of personal data, t~~ The legal basis for processing personal data should be established in accordance with the Regulation 2016/679, namely Article 6, 9 and 10 thereof. To the extent strictly necessary and proportionate for the purposes of compliance with a legal obligation according to this Directive to which entities, competent authorities, CERTs, CSIRTs, SPOCs, NIS CG, CSIRT Network and CyCLONe are subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in competent public authorities according to this Directive, the processing of personal data shall be considered lawful and in line with Article 6 (1) (c) or (e) of the 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 ~~the following~~ various types of personal data, such as: IP addresses, uniform resources locators (URLs), domain names, and email addresses.

(69a) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679

(69b) The processing of special categories of data as defined in Article 9 (1) of the Regulation (EU) 2016/679 is fobidden unless processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The security of network and information systems of essential and important entities should be considered as substantial public interest, therefore it is necessary to introduce in the Directive a legal basis for processing by competent authorities, SPOCs and CSIRTs special categories of data. Such processing should be made only to the extent that is strictly necessary and proportionate for the purposes of ensuring the security of network and information systems of essential and important entities. Specific measures to safeguard the fundamental rights and the interests of the data subject should be also introduced, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

(80) ~~In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making26 . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.~~

Articles

Article 2

Scope

(...)

~~3. This Directive is without prejudice to the~~ **responsibility** ~~competences of Member States concerning the maintenance of~~ ***regarding essential State functions*** ***concerning*** ~~public security, defence and national security~~ ***in accordance*** ~~in compliance with Union law.")~~

3.a This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.

(...)

5a. To the extent that is strictly necessary and proportionate for the purposes of ensuring the security of network and information systems of essential and important entities, competent authorities, SPOCs and CSIRTs may process special categories of personal data referred to in Article 9 (1) of Regulation (EU) 2016/679 subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

6. Where provisions of sector–specific **Union legal** acts ~~of Union law~~ require essential or important entities ~~either~~ to adopt cybersecurity risk management measures or to notify **significant** 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 provisions on supervision and enforcement laid down in Chapter VI~~, shall not apply **to those entities**. **Where the respective Union legal act containing such sector-specific provisions lays down corresponding rules on supervision and enforcement, Chapter VI should not apply to those entities either.**

7. In order to safeguard a coherent minimum standard of cybersecurity across all sectors, sector-specific Union legal acts referred to in paragraph 6 should include:

(a) cybersecurity risk management measures, that are at a minimum equivalent to those laid down in article 18 paragraphs 1 and 2 of this Directive; and

(b) requirements to notify significant incidents or cyber threats that are, at a minimum, equivalent to those laid down in article 20 paragraphs 1 through 4 and further include:

(i) where appropriate, automatic and direct access to the incident notifications by the national competent authority under this Directive through a common reporting mechanism; or

(ii) where appropriate, automatic and direct forwarding of the notifications to the national competent authority under this Directive or the national Computer Security Incident Response Teams designated in accordance with this Dircetive by the authority that receives incident notifications under the sector-specific Union legal act.

(c) requirements concerning cross-border cooperation for the relevant authorities shall be at least equivalent with those set out by this Directive.

8. The Commission shall periodically review the application of the equivalent effect requirement in paragraph 6 in relation to sector-specific provisions of Union legal acts. The Commission shall consult the Cooperation Group when preparing these regular assessments and developing the potential guidelines, recommendations on necessary actions or measures.

9. When additional sector-specific provisions pertaining to cybersecurity risk management measures and notification obligations appear to be necessary to ensure high levels of cybersecurity, the Commission should assess whether such provisions can be stipulated in an implementing or delegated act referred to in Article 18 (5) and (6) of this Directive. The Commission shall consult the Cooperation Group when preparing assessment.

Article 4
Definitions

(...)

~~(2)~~ 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any ~~action~~ **event** that **may** compromise**~~s~~** 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**, services** and information systems;

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

(5) 'incident' means any event that compromise or may compromise 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;

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

(16b) 'Qualified trust service provider' means a qualified service provider within the meaning of article 3(20) of Regulation 910/2014;

(…)

Article 5
National cybersecurity strategy

(…)

1.(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 [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and**~~,~~ ~~and~~** threats, especially cyber related**~~, and~~ as well as** the exercise of supervisory tasks**, as appropriate.**

(…)

Article 10
Requirements and Tasks of CSIRTS
(…)

3a. CSIRTs shall establish cooperation relationships with third countries national CERTs and CSIRTs and may exchange relevant, necessary and proportionate information in view of their tasks, which, in this context, can create an important reason of public interest

Article 11
Cooperation at national level

(...)

4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the **competent** authorities **designated** ~~responsible for critical infrastructure~~ pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive~~]~~**], the competent authorities under Commission Implementing Regulation 2019/1583, national regulatory authorities designated in accordance with Directive (EU) 2018/1972, the national authorities designated pursuant to Article 17 of Regulation (EU) No 910/2014,** ~~and~~ the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation~~]~~**], as well as competent authorities designated by future sector-specific Union legal acts** within that Member State.

5. Member States shall ensure that their competent authorities **under this Directive and the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]** regularly **exchange** ~~provide~~ information ~~to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]~~ on **the identification of critical entities,** risks, **threats and incidents, especially cyber related** 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 risks and incidents.

5.a For the purposes of simplifying the reporting of ~~security~~ incidents ~~which entail a possible personal data breach~~, Member States ~~shall~~may establish a single-entry point for all notifications required under this Directive, as well as under Regulation (EU) 2016/679 and Directive 2002/58/EC, where appropriate, when such incidentes entail a possible personal data breach. Member States may integrate notifications required under other sector-specific Union legal acts in the single-entry-point. This single-entry point shall not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to independent ~~suprvisory~~supervisory authorities.

5b. Member States shall ensure that their competent authorities under this Directive and the competent authorities designated pursuant to Regulation (EU) XXXX/XXXX [DORA Regulation] regularly exchange information on cybersecurity risks, cyber threats and incidents affecting essential entities who may be financial entities or critical third party ICT service providers, pursuant to Regulation (EU) XXXX/XXXX [DORA Regulation], as well as the measures taken by competent authorities in response to those risks and incidents.

5c Information covered by professional secrecy may not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law, including the exchange of information among competent authorities designated pursuant to Regulation (EU) XXXX/XXXX [DORA Regulation] or competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and competent authorities designated in accordance with Article 8 of this Directive.

5d Member States shall ensure that their competent authorities under this Directive and the supervisory bodies designated pursuant to article 17 of Regulation (EU) No 910/2014 regularly, and at least once per year, exchange information on cybersecurity risks, cyber threats and incidents affecting trust service providers.

5e The providers of public electronic communications networks or electronic communications services available to the public referred to in Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code shall cooperate, as appropriate, with competent authorities designated under this Directive.

Article 12

Cooperation Group

(...)

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(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group. **A meeting with the participation of ESAs shall be held regularly and, at least, once a year.**

4.(l) providing guidance and cooperating with the Commission on guidelines or recommendations on necessary actions or measures to be taken by the competent authorities designated under sector-specific Union legal acts in relation to the implementation of said legal acts in order to ensure consistency with provisions under this Directive.

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 promote strategic cooperation and **facilitate** exchange of information.

Article 18

Cybersecurity risk management measures

2. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network, **services** and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network, services and information systems appropriate to the risk presented.

1a. This Directive applies an "all-hazard" approach that includes the protection of network and information systems including the physical protection from relevant natural and man-made risks that could compromise 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.

(…)

5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications, **as well as sectoral specificities, as necessary,** of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

Article 21

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with ~~certain requirements of Article 18~~ **cybersecurity risk management measures,** Member States may require **all or certain groups of** essential and important entities to ~~certify certain~~ **use trust services or notified electronic identification schemes under Regulation 910/2014. Member States may also require entities to use particular categories of ICT products,** ~~ICT~~ **services and** ~~ICT~~ **processes certified** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881~~. The~~ **in order to demonstrate compliance or establish a presumption of conformity with certain requirements. The ICT** products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

2. The Commission shall be empowered to adopt ~~delegated~~ **implementing** acts specifying which categories of essential entities shall be required **to use certain categories of certified ICT products, ~~ICT~~ services and ~~ICT~~ processes or** obtain a certificate ~~and~~ under ~~which~~ specific European cybersecurity certification schemes **adopted pursuant to Article 49 of Regulation (EU) 2019/881**. ~~pursuant to paragraph 1The delegated acts shall be adopted in accordance with Article 36.~~ **When preparing the implementing act, the Commission shall:**

(i) take into account the impact of the measures on the manufacturers or providers of such ICT products, services or processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, services or processes;

(ii) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;

(iii) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, services or processes, particularly SMEs;

.

Article 29

Supervision and enforcement for essential entities

(...)

9. Member States shall ensure that their competent authorities **under this Directive** inform the relevant competent authorities **within that same** ~~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. **Where appropriate**, ~~Upon request of~~ competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]~~,~~ **may request** competent authorities **under this Directive** ~~may~~ **to** exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

10. Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum pursuant to Article 29 (1) of Regulation (EU) XXXX/XXXX [DORA] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity designated as critical ICT third-party service provider pursuant to Article 28 of Regulation (EU) XXXX/XXXX [DORA] with the obligations pursuant to this Directive.

Article 32

Infringements entailing a personal data breach

1. Where the competent authorities have information ~~indications~~ that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall**, without undue delay,** inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ~~within a reasonable period of time~~.

*Article ~~35~~**36***

~~Review~~

Exercise of the delegation

(…)

~~2.~~ **~~The Commission shall periodically review the application of the equivalent effect requirement in Article 2(6) of this Directive in relation to sector-specific provisions of Union legal acts. The Commission shall consult the Cooperation Group when preparing these regular assessments.~~The power to adopt delegated acts referred to in Articles 18(6) ~~and 21(2)~~ shall be conferred on the Commission for a period of five years from […]**

3. The delegation of power referred to in Articles 18(6) **~~and 21(2)~~** may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

(…)

Article 38

Transposition

1. Member States shall adopt and publish, by … [~~18~~ **24** months after the date of entry into force of this Directive, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].

(…)

Article 39

Amendment of Regulation (EU) No 910/2014

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

Article 40

Amendment of Directive (EU) 2018/1972

Articles 40 and 41 of Directive (EU) 2018/1972 are deleted **effect from… [date of the transposition deadline of the Directive].**

ANNEXES

With regard to trust service providers, a differentiation of the regulatory treatment between non-qualified and qualified trust service providers could be envisaged with the following proposed amendments in Annex I and II:

iii) **In Annex I point 8:- qualified trust service providers referred to in point (19) (20) of Article 3 of Regulation (EU) No 910/2014**

iv) **In Annex II point 6:- non-qualified trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014**

With regard to providers of public electronic communications networks, a precision of the regulatory treatment for micro and small enterprises could be envisaged with the following proposed amendment in Annex I and II:

ii) **In Annex I point 8: - Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972(26) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available. This is not applicable to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.**

In Annex II point 6a (new) Digital infrastructure - Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972(26) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available when they qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.