Council of the European Union

Brussels, 5 July 2021
(OR. en)

Interinstitutional File: 2020/0359(COD)

9583/2/21
REV 2

LIMITE

CYBER 171
JAI 689
DATAPROTECT 161
TELECOM 248
MI 447
CSC 238
CSCI 91
CODEC 850

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	14150/20
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 - Presidency compromise proposal on interaction of NIS 2 with sectoral legislation

Delegations will find attached the revised Presidency compromise proposal on NIS 2 interaction with sectoral legislation based on the written comments received from Member States. This revised proposal will be discussed at the HWPCI meeting of 7 July 2021. Changes compared to the previous version are highlighted in yellow**.** The changes compared to the Commission proposal are indicated in **bold** and strikethrough.

ANNEX

Recitals

(12) **This Directive sets out the baseline for cybersecurity risk management measures and reporting obligations across all sectors that fall within its scope. 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 reporting obligations appear to be necessary to ensure a high level~~s~~ of cybersecurity, ~~an assessment should be considered made by~~ the Commission should assess ~~as to~~ whether such provisions could be stipulated in an implementing act. Should such acts not be suitable for that purpose,** sector-specific legislation ~~and instruments could~~**an** contribute to ensuring **a** high level~~s~~ of cybersecurity, while taking full account of the specificities and complexities of ~~those~~ **the** sectors **concerned**. **At the same time, such sector-specific provisions of Union legal acts should duly take into account ~~of~~ the need for a comprehensive and ~~consistent~~ harmonised 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~~ **on** the Commission in a number of sectors, including transport and energy.

(12a) Where a sector–specific Union legal act **contains provisions** requir**inge**~~s~~ essential or important entities to adopt **measures of at least** ~~**an**~~ **equivalent effect to the obligations laid down in this Directive 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 a**~~**n**~~ **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 organisational 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**~~ **obligation to notify significant incidents and cyber threats should** ~~**(**~~**be at least equivalent with** ~~**/reflect at the minimum)**~~ **to the obligations set out in this Directive as regards the content, format and timelines of the notifications; (iii) the reporting modalities** ~~**by entities and the relevant o**~~ ~~**authorities**~~ **of sector-specific Union legal acts should** ~~**(**~~**be at least equivalent with to /reflect at the a minimum)**~~ **the requirements set out in this Directive as regards their content, format and timelines and should take into account the role of the CSIRTs; (iv) the cross-border cooperation requirements for the relevant authorities should** ~~**(**~~**be at least equivalent with to /reflect at the a minimum)**~~ **those set out** ~~**by**~~ **in 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 relevant provisions of this Directive should continue to apply to the entities not covered by those sector-specific provisions.**

The Commission should ~~regularly~~ **periodically review** **the application of the equivalent effect requirement in relation to sector-specific provisions of Union legal acts and** ~~may~~ **can** 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~~ **potential** **gaps** ~~with~~ **in relation to** ~~provisions under~~ **this Directive**. ~~relation to the implementation of the *lex specialis*.~~ The Commission ~~shall~~ **is to** consult the Cooperation Group when preparing the ~~regular~~ **periodical review** and developing **those**~~he~~ potential guidelines**, recommendations.**

(12aa~~**b**~~**)** ~~**Key**~~ **Sector-specific Union legal acts should take account of the** ~~**Key**~~ **definitions outlined in Article 4 of this Directive.** ~~**should serve as a baseline for sector-specific Union legal acts.**~~

(12ab~~**a**~~**)** **Where** **sector-specific provisions of Union legal acts require essential or important entities to adopt measures of at least** ~~**an**~~ **equivalent effect to the 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** **that** ~~**is**~~ **purpose,** ~~**the above-mentioned**~~ **those** **sector-specific provisions** ~~**may**~~ **can** ~~**provide for**~~**allow Member States to establish a common, automatic and direct reporting mechanism for notifying 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 a mechanism that ensures 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**~~ **of implementing the common, automatic and direct reporting mechanism, Member States can** ~~**-**~~**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~~ **out in** 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~~ **work of** ~~workings~~ of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive**,** ~~and~~ **as well as** 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~~ **can** cover the financial sector in their activities.

(13a) In order to avoid gaps between and duplications of cybersecurity obligations imposed on entities in the aviation sector referred to in point 2 (a) of Annex I ~~(2) (a),~~ competent authorities under Regulations 300/2008, 2018/1139 and this Directive~~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~~ can be considered by the competent authorities under Regulations 300/2008 and 2018/1139 ~~Commission Implementing Regulation 2019/1583 as~~ compliant with the requirements laid down in ~~that~~ Commission Implementing Regulation 2019/1583.

(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~~ as 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. Competent 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 relevant 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~~ activities 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 minimise the administrative burden for the entities concerned, 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**~~ **can request** competent authorities under this Directive ~~should be allowed~~ to exercise their supervisory and enforcement powers ~~on~~ **in relation to** an essential entity identified as critical. ~~Both~~ **Competent authorities under both Directives** should cooperate and exchange information for th**at** purpose.

(14a) Union law on the protection of personal data and privacy applies to any processing of personal data ~~falling within the scope of~~ under 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 Council[18], 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 of 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 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 State~~s~~, 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.

For that purpose, Member States ~~may~~ can determine that competent authorities under this Directive or national CSIRTs are the 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 under~~The sector-specific Union legal acts which require cybersecurity risk management measures or ~~notification~~reporting obligations of at least equivalent effect with those laid down in this Directive ~~sector -specific lex specialis may~~ could provide that their designated competent authorities ~~a~~exercise their supervisory and enforcement powers in relation to such measures or obligations with ~~exercise the supervision and enforcement over as regards obligations given provided for in those sector specific lex specialis with~~ the assistance of the competent authorities designated in accordance with this Directive. ~~In order to achieve this, t~~The competent authorities concerned ~~should~~ could establish ~~effective~~ cooperation for this purpose. Such cooperation ~~shall cs~~hould include, 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 a mechanism for the exchange of information between competent authorities, including access to information requested by competent authorities 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 purposes of their tasks. Such disclosure or~~ The exchange of such personal information that is considered necessary for the purposes of mitigating significant cyber threats and responding to an ongoing significant incident could be considered an ~~may constitute~~ important reasons~~ of public interest.**

(40) Risk-management measures should **take into account the degree of dependence of the entity on network and information systems and and focus particularly on the networks and information systems which the functioning of the services the entity is regulated for depend on. They should** include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.

(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 unauthorised 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 those included in the ISO 27000 series. Those measures should be ~~in line~~coherent with Directive XXXX [CER Directive].

(44a) National competent authorities, in the context of their supervisory tasks, may also benefit from MSSP services such as security audits and penetration testing. To assist entities as well as national competent authorities in selecting skilled and trustworthy MSSPs, the Commission with the assistance of the Cooperation Group and ENISA, should consider the possibility of establishing relevant EU certification schemes, where appropriate under the Regulation 2019/881.

(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**s** on th**o**se 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**s** 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~~ **should 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. Based on the work already done, ENISA ~~may~~ can also provide further guidance ~~documentation~~ on security and reporting requirements ~~arrangements~~ for providers of public electronic communication networks or publicly available electronic communication services ~~entities that were subject to obligations from under Directive (EU) 2018/1972~~ to facilitate harmonisation, transition and minimise disruption. Member States ~~may~~ can 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 purpose~~s~~ 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 pProcessing of personal data by competent authorities, SPOCs and CSIRTs should be laid down inor 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 in the exercise of official authority vested in the data controller, as referred to in Article 6(1) point (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.

Processing of personal data by competent authorities, SPOCs and CSIRTs should be laid down in 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 in the exercise of official authority vested in the data controller, as referred to in Article 6(1) point (c) or (e) of Regulation (EU) 2016/679.

(69a) Competent authorities, SPOCs and CSIRTs can, to the extent that is strictly necessary and proportionate for the purpose of ensuring the security of network and information systems of essential and important entities, process special categories of personal data in accordance with Article 9~~(1)~~ of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

Articles

Article 2

Scope

(...)

3a **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.**

~~To the extent that is 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~~ such entities**. **~~Where the respective sector-specific Union legal act containing such sector-specific provisions lays down corresponding rules on supervision and enforcement, Chapter VI of this Directive should shall not apply to those such entities either.~~ If sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive should continue to apply to the entities not covered by those sector-specific provisions.**

~~7.~~ The requirements referred above in this paragraph shall be considered equivalent in effect to the obligations laid down in this Directive if ~~aIn order to safeguard ensure a coherent minimum standard of cybersecurity across all sectors, sector-specific Union legal acts referred to in paragraph 6 should~~ shall 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; or

(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~~ to (4) ~~(6)~~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, where appropriate; 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 TeamsCSIRTs designated in accordance with this Directive by the authority that receives incident notifications under the sector-specific Union legal act, where appropriate.~~

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

~~7~~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 those ~~regular assessments~~ periodical reviews ~~and when 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 a high levels of cybersecurity, the Commission should shall assess whether such provisions can be stipulated in an implementing act or a delegated act referred to in Article 18 (5) and (6) of this Directive.**~~

Article 4
Definitions

(...)

~~(2)~~ 'security of network~~, services~~ and information systems' means the ability of network**,** **services** 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 ~~**data**~~ 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 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 trust service provider within the meaning of Aarticle 3(20) of Regulation (EU) No 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 **cybersecurity risks,** cyber threats **and incidents as well as on non-cyber risks, threats and incidents and** the exercise of supervisory tasks**, as appropriate.**

(…)

Article 10

Requirements and Tasks of CSIRTs~~S~~

(…)

3a. CSIRTs may ~~shall~~ establish cooperation relationships with national CERTs and CSIRTs of third countries. As part of this cooperation, they ~~and~~ may exchange relevant, ~~necessary and proportionate~~ information, including personal data in accordance with Union law on data protection. ~~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, the 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~~ 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. **Member States shall also ensure that competent authorities under this Directive regularly exchange relevant information with competent authorities designated under Regulation (XXXX/XXXX)[DORA Regulation], Directive 2018/1972 and Regulation (EU) 910/2014.**

5a For the purpose~~s~~ 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~~ potential ~~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 Aarticle 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) **point** (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, recommendations on necessary actions or measures to be taken by the competent authrorities designated under sector-specific Union legal acts in relation to the implementation of said those legal acts in order to ensure consistency with provisions under this Directive.**~~

~~**4.(m) adopting security rules on the protection of classified information and sensitive non-classified information in accordance with security principles and rules laid down in Commission Decisions 2015/443 and 2015/444 in connection with information sharing on cybersecurity risks, threats and incidents between the arrangements set out in Article 26 of this Directive and arrangements under Article 40 of Regulation (EU) XXXX/XXXX [DORA Regulation].**~~

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. 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.

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.

(…)

~~6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.~~

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 (EU) No 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.**~~

Article 21a

Use of trust services or notified electronic identification schemes

In order to demonstrate compliance with ~~certain requirements of Article 18~~ cybersecurity risk management measures referred to in Article 18, 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 (EU) No 910/2014.

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~~ **in relation to** an essential entity identified as critical or equivalent.

Article 32

Infringements entailing a personal data breach

1. Where the competent authorities have ~~indications~~ ~~**evidence**~~ **established** that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 **of this Directive** 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.~~**

(…)

Article 38

Transposition

1. **By … [~~18~~ 24** months after the date of entry into force of this Directive**],** 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

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

Article 40

Amendment of Directive (EU) 2018/1972

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

Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359 (COD)

Brussels, 29 July 2021

WK 9834/2021 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 8685/21 14150/20
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 - Revised Presidency compromise proposal on interaction of NIS 2 with sectoral legislation: Comments by the CZ delegation

Delegations will find in Annex comments by the CZ delegation on the second revision of the Presidency compromise proposal on interaction of NIS 2 with sectoral legislation.