Council of the European Union

Brussels, 9 June 2021
(OR. en)

9583/21

Interinstitutional File:
2020/0359(COD)

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

Member States will find in Annex the Presidency compromise proposal on NIS 2 interaction with sectoral legislation based on the written comments received. In addition to the compromise proposal, Member States will find, at the end of this document, a number of questions concerning DORA, EECC and eIDAS for which the Presidency requests further guidance from Member States before coming forward with concrete drafting proposals. Member States are kindly asked to submit their answers to these questions by 17th June, COB to bcp@reper-portugal.be and WP-CYBER@consilium.europa.eu.

ANNEX

Presidency Compromise Proposal 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 obligations appear to be necessary to ensure high levels of cybersecurity, an assessment should be considered as to whether such provisions can 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** 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 with 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 entities and the relevant authorities should be at least equivalent with the requirements set out in this Directive as regards their content, format and timelines; (iv) the cross-border cooperation requirements for the relevant authorities should be at least equivalent with 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 in **this regard.** ~~relation to the implementation of the *lex specialis*.~~ **The Commission should consult the Cooperation Group when preparing the regular assessment and developing the potential guidelines.**

(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 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 a common, automatic and direct reporting mechanism for significant incidents and cyber threats to the authorities whose tasks are set out in the respective sector-specific provisions and the competent authorities responsible for the cybersecurity tasks provided for in this Directive or for an automatic and direct mechanism that ensures timely sharing of information and cooperation among the relevant authorities concerning such notifications.

(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 designated under this Directive. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.

(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 affecting critical entities or **entities equivalent to critical entities** as well as on the cybersecurity 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 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.

(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**. 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 Dircetive.** ~~which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.~~

(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 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 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.

(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.

(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 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 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 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.

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 provision**s** on supervision and enforcement laid down in Chapter VI, shall not apply **to those entities**.

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 compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

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 the exercise of supervisory tasks**, as appropriate.**

(...)

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] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation] 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 cybersecurity risks, cyber 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 establish a single-entry point for all notifications required under this Directive, Regulation (EU) 2016/679 and Directive 2002/58/EC. 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 authorities.**

Article 12

Cooperation Group

(...)

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 21

Use of European cybersecurity certification schemes

1. ~~In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The 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 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 1~~The delegated acts shall be adopted in accordance with Article 36.

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 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.

Article 32

Infringements entailing a personal data breach

1. Where the competent authorities have 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

Review

(…)

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. 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 **with effect from… [date of the transposition deadline of the Directive].**

Questions to Member States on DORA, EECC and eIDAS

DORA

In the opinion of the European Central Bank of 04 June 2021 (document 9530/21) the following points were raised concerning interaction between the NIS 2 proposal and DORA:

"The ECB understands that the proposed regulation represents, in relation to financial entities identified as operators of essential services, sector specific legislation (lex specialis) in accordance with the meaning as set out in Article 1(7) of Directive (EU) 2016/1148 of the European Parliament and of the Council (hereinafter the 'NIS Directive'); this implies that the requirements under the proposed regulation would, in principle, prevail over the NIS Directive. In practice, financial entities identified as operators of essential services would, inter alia, report incidents in accordance with the proposed regulation rather than the NIS Directive. While the ECB welcomes the reduction of potential overlapping requirements for financial entities in the field of incident reporting, further consideration should be given to the interplay between the proposed regulation and the NIS Directive. For example, under the proposed regulation an ICT third-party service provider could be subject to recommendations issued by the lead overseer. At the same time, the very same ICT third-party service provider may be classified as an operator of essential services under the NIS Directive and be subject to binding instructions issued by the competent authority. In such case, the ICT third-party service provider could be subject to conflicting recommendations issued under the proposed regulation and binding instructions issued under the NIS Directive. The ECB suggests that the Union legislative bodies reflect further on potential inconsistencies between the proposed regulation and the NIS Directive that may hamper the harmonisation and reduction of overlapping and conflicting requirements for financial entities.

The ECB also understands that under the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/11489 (hereinafter the 'proposed NIS2 directive'), 'near misses' will be subject to reporting obligations. While Recital (39) of the proposed NIS2 directive refers to the meaning of the term 'near misses', it is unclear whether the intention is to require that near misses be reported by the financial entities listed in Article 2 of the proposed regulation. In this regard, and also taking into account that near misses can only be identified as such after they have occurred, the ECB would welcome receiving notification of significant near-misses in a timely manner, as is currently the case for cyber incidents. The ECB suggests that there should be greater coordination between the proposed regulation and the proposed NIS2 directive to clarify the exact scope of reporting to which any given financial entity may be subject under these two distinct but connected pieces of Union legislation. At the same time, 'near misses' would need to be defined and provisions clarifying their significance would need to be developed.

The ECB welcomes incentivising financial entities to share on a voluntary basis cyber threat intelligence information amongst each other to enhance and bolster their cyber resilience postures. The ECB itself has assisted with the market-driven Cyber threat Intelligence Information Sharing Initiative (CIISI-EU) and has made available the blueprints for anyone to build and foster such an initiative.

The ECB supports cooperation between the competent authorities for the purposes of the proposed regulation, the European Supervisory Authorities (ESAs), and the Computer Security Incident Response Teams (CSIRTS). It is essential to exchange information in order to ensure the operational resilience of the Union, as information sharing and cooperation among authorities can contribute to the prevention of cyber-attacks and help reduce the spread of ICT threats. A common understanding of ICT-related risks should be promoted and assessing such risks in a consistent manner should be ensured across the Union. It is of utmost importance that information be shared with the single point of contact and the national CSIRTS by competent authorities only when there are clearly established classification and information sharing mechanisms, coupled with adequate safeguards to ensure confidentiality."

Q1: Concerning cooperation between the competent authorities for the purposes of the proposed regulation, the European Supervisory Authorities (ESAs), and the Computer Security Incident Response Teams (CSIRTS), are Member States satisfied with the compromise proposal on DORA? Is further clarification necessary in the NIS2 proposal? The Presidency would appreciate concrete text proposals in this regard.

Q2: Are Member States satisfied with how NIS authorities can be involved in the oversight framework under the current compromise proposal on DORA? Is further clarification in this respect necessary in the NIS2 proposal? The Presidency would appreciate concrete text proposals in this regard.

Q3: In order to achieve a stringent and harmonised NIS echo system, it is important that the two frameworks (NIS 2 and DORA) are consistent in relation to the definition and reporting of cyber threats. Do Member States agree, as respective negotiations of both legal acts move forward, on the necessity of alignment of both frameworks in this respect? The Presidency would appreciate concrete text proposals in this regard.

eIDAS and EECC

Concerning article 39 [Amendment of Regulation (EU) No 910/2014] and article 40 [Amendment of Directive (EU) 2018/1972], during the read-through of the proposal on NIS2, Member States have indicated that further discussion and analysis of these articles would be merited in order to fully understand their potential impact.

Furthermore, Member States have stated that it is imperative to view the revised NIS Directive proposal as the horizontal framework for cybersecurity in the EU and that it should serve as a baseline standard for minimum harmonisation of all relevant sectoral legislation in this field.

Q4: With a view to ensure that the revised NIS Directive indeed serves as the horizontal framework for cybersecurity in the EU, that legislative fragmentation through lex specialis is kept to a minimum and in order to ensure consistency of the legislative framework and to promote clarity and avoid unnecessary duplication of obligations on operators, would additional clarification or the introduction of supplementary safeguards in the NIS2 proposal be required in order to ensure the continuation of current practices and build on the knowledge and experience gained in Directive (EU) 2018/1972? The Presidency would appreciate concrete text proposals in this regard.

Q5: Does the proposal for amending Regulation (EU) No 910/2014 sufficiently cover with compensating provisions Member States' concerns in relation to Article 39 on the NIS 2 proposal? If not, would additional clarifications in the NIS 2 proposal be required? The Presidency would appreciate concrete text proposals in this regard.