TABLE OF CONTENT

AUSTRIA

General position

In recent years, cyber-attacks and incidents have shown that it is fundamental to further enhance the level of cybersecurity. Thus, we welcome the fact that the Commission tabled a new Directive on measures for a high common level of cyber security in the Union. Overall, we see the potential of NIS 2 to address cybersecurity in a comprehensive way, addressing short-comings and experience gained from NIS 1 as well as developments that took place in the threat and policy landscape.

It is key that the resilience against cyber-attacks is increased on a national as well as Union wide basis. The NIS 2 Directive should increase the level of cybersecurity across the economy. In addition, NIS 2 should provide a framework where Member States can enhance and deepen their cooperation at EU level, in particular in the event of large-scale incidents or cyber crises. In that regard, we welcome the fact that building trust and sharing information are an integral part of NIS 2 Directive.

EU cybersecurity policy must continue to be designed with the aim of strengthening user-trust in digital products and services and enabling a strong and effective digital single market. On the other hand, over-regulation and double burdens must be avoided. NIS 2 should provide a framework for cooperation on cybersecurity matters, between the Member States, Member States and the EU and the private sector.

Detailed position on interaction of NIS2 with Sectoral Legislation

AT shares the view that the NIS 2 Directive should act as the main horizontal cybersecurity instrument, serving as a strong legal basis, providing a robust framework for national and Union wide strategic, operational and technical cooperation.

While it can be certainly of merit to address sector-specific aspects – as threats, ICT equipment and security measures may vary broadly depending on the sector –, there should be a baseline of security requirements for all sectors in order to achieve a common level of cybersecurity. This baseline should be anchored in the NIS 2 Directive, spanning across all sectors where services which are key for the society and economy as whole. To that end, AT welcomes the fact that NIS 2 provides for more harmonized security requirements on the one hand, while providing for a legal basis to address sector-specific requirements at second level legislation on the other hand.

The latter is key for a particular reason. Despite the fact that sector-specific requirements can be stipulated in sectoral legislation in an efficient way, sectoral legislation may lead to fragmentation when not taking into account the horizontal cybersecurity requirements.

Moreover, sectoral legislation may lack of the robust governance framework that NIS established. Sector-specific requirements alone will not increase the level of cybersecurity when provisions on the evidence of implementation, the regularity of audits and/or enforcement are disregarded. On top of that, not all sectoral authorities may be in a position to enforce the rather complex matter of cybersecurity. Even if the addressees have to provide evidence of implementation through third-party audits, (non-cybersecurity) authorities may find it challenging to assess the quality of these audits. Thus, whenever there is a discussion on lex specialis, evidence of implementation and enforcement powers and capabilities of sectoral authorities should be taken into consideration.

Sectoral legislation regulating the notification of incidents and threats may lead to a silo-effect with regard to creating common situational awareness and cross-border cooperation. Common situational awareness must be achieved e.g. by requiring sectoral authorities to forward notifications immediately or by providing opening clauses in sectoral legislation to solve this on national level accordingly. Only then cross-border cooperation in particular in the CSIRTs network and CyCLONe can be ensured too.

Lex specialis clause: For AT, it is currently unclear what "at least equivalent" means (would the ECJ be the ultimate competent authority to judge this?). It would make sense to specify the relevant criteria concerning the term “at least equivalent” within the lex specialis clause. This should not only cover the security requirements, but also the content of notifications, the time limit for notifying threats or incidents (in order to avoid fragmentation in incident handling), the enforcement mechanisms and supervisory powers. It should be noted that sectoral-legislation should not be proposed if existing instruments, such as the NIS Directive, can adress the sectoral specificities by means of implementation already.

Drafting suggestion for lex specialis clause in Art 2(6) [in bold and underlined]

“Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply. **Cybersecurity risk management measures of sector–specific acts of Union law are at least equivalent in effect if they entail all requirements according to Art 18, in particular of Art 18(2) and (3), and if they adress sectoral specificities. Reporting obligations of sector–specific acts of Union law are at least equivalent in effect if they contain all requirements and proceudres of Art 20, including, but limited to the significance of the incident or threat, the time limit to notify, the content of the notification, the procedure of the notification (including a final report), a response to the notifying entity (Art 20 para 5), including initial feedback, a cross-border notification mechanisms (Art 20 para 6), a publication procedure (Art 20 para 7). Provisisons on cybersecurity risk management measures or notificatoin of incidents or significant cyber threats are not at least equivalent in effect if the provisisons on supervision and enforcement of the obligations set out in the sector–specific acts are less comprehensive, effective and dissuasive than Chapter VI.**”

Detailed position on to sectoral legislation referred to in NIS 2

- **eIDAS:** AT is concerned that transferring Art. 19 of eIDAS regulation into a directive poses a major legal challenge. A division of responsibility for trust service providers (TSPs) in general and qualified TSPs will lead to problems, as security measures that qualified TSPs have to take according to Art. 19 and 24 eIDAS Regulation are mostly based on the same proven technical standards. It would hardly be possible to determine compliance with requirements under Art. 24 eIDAS Regulation without also assessing compliance with requirements under Art. 19 eIDAS Regulation. Conflicts of competence could hardly be ruled out in the case of an assessment by different authorities.
  Security measures that TSPs would have to take according to Art. 18 of the proposed NIS 2 Directive include only a part of the security measures to be taken according to Art. 19 of the eIDAS Regulation (in particular with regard to parts of a trust service that do not concern the TSP’s network and information systems, e.g. the identification of physically present persons by means of an official photo ID).
  Moreover, information that must be notified to eIDAS authorities according Art. 19 is essential for eIDAS authorities to perform their supervisory tasks. Without additional requirements at national level, security incidents would no longer be reported to the supervisory body but to a CSIRT or NIS competent authority. The supervisory body relies on information about security incidents, but reporting requirements to different authorities could prove to be an additional hurdle.

Additional problems can arise with the trusted lists that each member state has to keep. The cryptographic keys used for this cannot be transferred to another authority at will either, as they are bound to a specific authority by published certificates.
Since the new eIDAS regulation is not yet tabled, it is impossible to assess whether there are compensating provisions to that problem. Given the fact that eIDAS is a highly specialized and interwoven governance system as such, it should be assessed whether the new eIDAS regulation could not include a provision according to which eIDAS authorities must forward incident notifications to NIS authorities.

- **EECC:** Since the security related provisions enshrined in the EECC are legally almost identical to the ones in the NIS Directive and given the strong overlap with regard to telecom, cloud, DNS etc., transferring the EECC provisions to NIS seems plausible.

- **CER:** There should be more clarity on how "genuine" physical security measures and physical security as part of cybersecurity relate to each other (preferably in a recital) in order to avoid potential conflicts of competence of CER and NIS authorities.
    - **Harmonization**
      With the purpose of a maximum harmonization of CER and NIS 2 for entities subject to these directives, we suggest to have a discussion on the following key terms: essential services, critical entities, essential entities, important entities
    - **National Strategy**
      Art 3 CER / Art 5 NIS 2: We fully support the suggestion to have a policy framework in place, which specifies the coordination between CER and NIS2 authorities for the purpose of information sharing. However, we would suggest to embed the policy framework either in the national cybersecurity strategy or the national strategy on CER. The reason being that if the strategies enter into force in different years the policy framework might become outdated. We would therefore propose to leave the obligation to make such policy framework in the NIS2 directive and only make a reference to it in the CER directive
    - **Identification of critical entities**
      Art 5 CER Directive foresees the need of CER authorities to identify for each sector and subsector referred to in the Annex, other than points 3, 4 and 8 thereof, the critical entities. Para 4 provides that NIS 2 authorities need to be informed of the identification of critical entities. Under the NIS 1 regime the identification of critical entities already took place and we would suggest to make a reference here to this identification process under NIS 1.
    - **Critical entities of particular European interest**
      We believe that the reasoning behind Art 14 CER (defining critical entities of particular European interest) is very important and should to a certain extent also apply to NIS 2. We would recommend to include the need for information sharing and enhanced cooperation of NIS 2 and CER authorities on this matter in Art 14 CER. **We would also like to encourage a discussion on whether an equivalent of Art 14 CER could/should be included in NIS 2.** The inclusion of such an Article should be without prejudice to the responsibility and jurisdiction of MS to supervise these entities.

- **DORA:** DORA includes a set of detailed sector-specific provisions and a robust governance framework but carried the risk of creating a silo in one of the most relevant sectors. The negotiations on DORA, however, have born good examples on how to overcome this risk when enacting sectoral legislation. To be more precise, the current compromise proposal entails provisions allowing the national legislator to determine to whom incident information could be forwarded. In addition, it includes detailed provisions on cooperation between DORA and NIS authorities at national and EU level.
  The remaining concern is that not all DORA authorities may have the capabilities or capacities to provide guidance to supervised entities affected by an incident in the same way as CSIRTs or NIS authorities do. Moreover, information on cyber threats might be less valuable for DORA authorities in comparison to CSIRTs.
  An issue where we see some uncertainty is the relationship of the new oversight framework of critical ICT third-party service providers (Art 28 DORA) with the supervisory powers of NIS competent authorities in the sector digital infrastructure. For instance, cloud service providers that are essential entities under NIS 2 as well as designated as critical ICT third-party service providers under DORA could be subject to requests for information, investigations and on-site inspections by both NIS competent authorities and DORA lead overseer at the same time with the result of possibly diverging recommendations in the aftermath. In this regard, the WP dealing with DORA is still assessing the possibility of how NIS authorities can be involved in the oversight framework.

- **Commission Implementing Regulation 2019/1583:** The Implementing Regulation 2019/1583 lays down cybersecurity measures with regard to aviation security. It should be noted that the scope of the Implementing Regulation is enormous, covering all airport operators, air carriers and entities as defined in the national civil aviation security programme. Having in mind that aviation security (protection from unlawful interference) is narrower than the broad terms of risk and incident according to NIS, lex specialis will likely not be applicable, resulting in a complicated scenario where the AVSEC authority may replace compliance with the requirements of the Implementing Regulation 2019/1583 by compliance with NIS in order to avoid double-burden for airport operators and air carriers. On top of that, EASA is working in parallel on common requirements for Information Security Management Systems (ISMS) and reporting of cybersecurity incidents which may impact aviation safety. Likewise, aviation safety is narrower than NIS which is why lex specialis will likely not be applicable either. Thus a double-burden to notify incidents (once to aviation safety authority, once to NIS authority) will arise. Moreover, airport operators and air carriers will be subject to three differenct EU cybersecurity requirements (NIS, Implementing Regulation 2019/1583 and EASA rules), making it very difficult to coordinate at national level and leading to an unclear situation for airport operators and air carriers.
  We strongly encourage to have an in-depth discussion in the HWP on this excessive legislative activity in the aviation sector.

BULGARIA

/The comments provided do not contain an exhaustive position on the matter and are without prejudice to any further development/

- *Proposal for regulation on digital operational resilience for the financial sector*[1] */DORA Regulation/*

  Bulgaria supports the genera concept of the approach taken to amend DORA Regulation and to include reporting to CSIRTs for major cyber incidents and significant threats. To avoid any misunderstanding, **recital 23 of NIS2** should be amended correspondently. At the same time, it is of vital importance the text of the "lex specialis" nature of DORA to be kept in order to not create confusion for the entities which is the legislation that prevails.
  In order MSs to comply with the requirements of article 11, para 4, we would suggest an amendment in **article 12, para 3 of NIS2** that not only the European Supervisory Authorities may participate in the activities of the Cooperation Group, but that the national competent authorities in the sense of DORA regulation should take part as well.

- *Cybersecurity Act*[2]

  Article 21 – Use of cybersecurity certification schemes
  Paragraph 1

  According to our assessment, the legal interpretation of article 56, para 2 of the CSA already allows MSs to require mandatory certification under their national law. In this regard, we do not see the purpose of the paragraph to be in an article, part of the legislative text, but rather **move it in a recital**. Nevertheless, based on the various discussions we have had with stakeholders, it creates a lot of ambiguity for the private sector and uncertainty for the fragmentation in EU as this article suggests that MSs, but not the EU will require this mandatory certification.

  Paragraph 2
  We would suggest paragraph 2 to be **deleted**.

  Bulgaria would like to thank the Commission for its explanations regarding the correlation of article 21, para 2 and the CSA during a HWPCI meeting held on 14th April 2021. We duly noted the explanation for the compliance between the two pieces of legislation. Nevertheless, we would propose the suggestion for the deletion of this paragraph as we believe that the first step in this process should be having the Commissions' assessment, by 31 December 2023, of a specific European cybersecurity certification scheme to be made mandatory. Having the full national support for the certification process and its importance for the high level of cybersecurity across the Union, we believe that the Commission's empowerment to adopt delegated acts for which categories of essential entities would be required to mandatory certification, can be premature at this stage and we would propose to follow the outlined framework of the CSA.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595
2 https://eur-lex.europa.eu/eli/reg/2019/881/oj

- *Proposal for directive on the resilience of critical entities*[3] */CER Directive/*
  As a general comment Bulgaria would like to express a concern that two different frameworks and respectively competent authorities would regulate a similar subject matter (security) for the same scope of entities (Annex 1 of NIS2). Bulgaria would like to stress that any misunderstanding for the entities regarding under which supervision they have requirements to comply, must be avoided.

  Security of critical infrastructure/essential entities in many cases should be taken in a holistic manner. For example, "entities in the digital infrastructure sector are in essence based on network and information systems and fall within the scope of the NIS 2 Directive, which also addresses the physical security of such systems as part of their cybersecurity risk management and reporting obligations. At the same time, the CER does not rule out the possibility that specific provisions could be applied to them". (Opinion of the European Economic and Social Committee, 8416/21).

  In the cases where MSs would have two competent authorities to regulate the risk imposed by the two directives – one for physical, one for digital – we believe the businesses and entities might experience difficulties based on the division of regulatory powers. This is extremely the case in relation to the notification of **incidents → article 13 of CER directive and article 20 of NIS2 directive.** Any doubt of when a critical entity shall report an incident to the competent authority under CER and when to the competent authorities under NIS2 should be avoided. This is highly sensitive having in mind the sanctions regime under NIS2. How entities such as the ones in digital infrastructure sector would be able to correctly define which framework the incident is falling under? The **definition** of incident in **article 2, paragraph 3 of CER** has a broad concept and we would call for discussion on a scenario where the definition for an incident in article 4, paragraph 5 of NIS2 might be interpreted in the light of CER directive and vice versa.

- *European Electronic Communications Code*[4] */EECC/*

  The impact of the deletion of article 40 and article 41 is still under ongoing assessment. Nevertheless, we would like to stress the following:

  - The difference between the **definition of "incident"** under NIS2 (art. 4, para 5) and EECC (art**. 2, para 42) is leading** to ambiguity and legal uncertainty. An assessment should be conducted how to smoothly transition the implementation from EECC to NIS2, especially having the fact that EECC has recently being transposed in the national legislation frameworks. Therefore, we would prefer to use simply a reference to Art. 2, item 21 of the EECC. We would insist on keeping the definition for "security incident" as in Art. 2, item 41 of the EECC to avoid ambiguity and excessive burden with the notion of "any event" with doubtful effects. What NIS 2 Directive could do in terms of "security incident" is to specify how the actual adverse could be assessed, but without replacing the by the more ambiguous "any event";

    Note: we would propose the definition of "security incident" within the meaning of art. 2, para 42 of the EECC to be kept only for the specific sector in relation to Annex 1, and not the proposal of NIS2 as a whole.

3 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN
4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG

- **Recital 54 of NIS2** (end-to-end encryption): we would encourage to not open a discussion on this point due to the heavily reached compromise during EECC negotiations;

- Further assessment of **article 18 of NIS2** is needed in relation to the impact to the providers of electronic communications networks and services (NB-ICS; NI-ICS and social networks) – are all requirements valid for all categories of services provided? We believe that we need a level playing field and proportionality in this regard.
- **Reporting obligations**: We prefer more clarity to whom and what needs to be notified, also, when. As regards the deadlines for reporting, the 72-hour option for reporting as per the GDPR seems relevant to us.

Considering that EECC was recently transposed on national level, as a general comment, we would like to stress the importance of a smooth transition to the requirements of NIS2, avoiding unnecessary costs and administrative burden.

- *eIDAS Regulation*
  In order to avoid any premature judgement, we would provide comments for the correlation between NIS2 and eIDAS after the publication of the new eIDAS proposal.

- *Directive 97/67/EC of the European Parliament and of the Council18, as well as express and courier delivery service providers*[5]
  - **Postal service providers**

  - Recital (19) of NIS2 states that postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council, 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 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.

  - Justification:

  - The proposed recital seems too ambitious and not in line with the Postal Services Directive (*Directive 97/67/EC, as amended by* Directives 2002/39/EC and 2008/6/EC) where such requirements do not exist.

  - We appreciate that the proposal foresees a general exclusion of micro and small entities from the NIS2 scope and a lighter ex-post supervisory regime applied to a large number of the new entities under the revised scope (so-called important entities). However, the degree of digitalisation of postal services and processes varies considerably also among SMEs in the postal sector and in particular, providers of universal postal service. Therefore, we would prefer to add the currently existing criterion in the NIS Directive about the degee of dependence of postal processes on network and information systems. Moreover, the proposed recital does not distinguish between categories of postal items such as as letters and parcels. In this regard, the obligation seems also excessive as it does not reflect the current trends of the postal sector of a constantly declining letters-mail' market.

5 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31997L0067

- *DNS, TLD registries and entities providing domain name registration services for the TLD*

a) Art. 4 (13) of NIS 2

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

- However, we are of the view that the following definition would be more appropriate: 'Domain Name Registration Services' means services provided by a domain name registrar, domain related security providers, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names.

- Justification:

- We would prefer a broader and clearer definition that involves all actors involved in collecting, processing, storing and transferring domain name registration data.

- *Changes related the "WHOIS data"*

a) Proposed changes:

- Whereas 59

- Maintaining accurate, verified and complete databases of domain names and registration data (so called "WHOIS data") and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, so that third-party rights such as intellectual rights could be protected and which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.

b) In Art. 23, para 1, after the word "accurate", we would like to add the word "verified"

c) In Art. 23.4, we propose the following:

- Member States shall ensure that the TLD registries and the registrars make available to the public, without undue delay, but no later than 24 hours (or other more feasible, but avoiding without undue delay as it is too undefined), after the registration of a domain name, fees and domain registration data which are not personal data.

- Justification: transparency is very important for us, the accurate, verified and complete databases, as well.

d) Other proposed changes in Art. 23

- We are wondering why the reference in Art. 23 is made only to TLD registries. We would like to refer explicitly not only to TLD registries, but also to registrars as the latter could be various legal entities and at the same time, the term "registrars" is more commonly used. Therefore, instead of "entities providing domain name registration services for the TLD", we would propose to use the common term "registrars" in Art. 23.

e) We would like to discuss the possibility to include a provision, it could be in a recital if not in the body itself, for the co-operation with ICANN's ongoing work to develop generic top-level domain (gTLD) policies, to ensure maximum access to domain name registration data for legitimate interests when possible/where appropriate under GDPR.

f) As a more general comment, we would like the new Directive to ensure that all WHOIS data is available to legitimate access seekers and for the moment, the proposed texts in Art. 23 in this regard are acceptable for us.

CZECH REPUBLIC

EECC

EECC has proven to be a good framework to address the security threats posed to electronic communications sector. In our view, the security aspects of electronic communications sector are highly specific, complex and form part of a wider regulatory EECC framework which by a sole derogation of Art. 40 and 41 EECC would erode. While we acknowledge that the security of electronic communications sector is of great interest of NIS authorities and they should participate in enhancing the cybersecurity practices of electronic communications sector entities, we think that **the basis for (not only cyber) security-related obligations addressed to electronic communications sector should remain in Art. 40 and 41 EECC** and the primary responsibility for ensuring high level of security of electronic communications sector entities should continue to lie with EECC authorities which shall closely cooperate with the NIS authorities.

In practice, the security measures under EECC comprise of measures aimed at protection of networks against disruptions caused by electromagnetic interference and processing loading or measures aimed at protection of interoperability of services. All of these are non-cyber measures would remain unaddressed if the Art. 40 and 41 were solely derogated. Furthermore, our EECC authority deals, on a daily basis, with incidents caused by human errors during the operation of equipment or facilities, system failures, natural phenomena or of similar nature. Such incidents represent a majority of incidents reported by electronic communications sector entities to our EECC authority. We believe that there is not much of an added value in notifying CSIRTs or NIS authorities about such incidents. As a matter of fact, given the large number of entities from electronic communications sector, administrating such types of incidents would be a considerable additional burden for CSIRTs operation.

If the Art. 40 and 41 were derogated, it would be necessary to ensure that non-cyber risks are duly addressed in the EECC framework. In addition, we would suggest reconsidering inclusion of number-independent interpersonal communication services into the essential entities' category.

eIDAS

In general, we think that the current regulatory regime related to the security of trust service providers in eIDAS is well-functioning and by the sole derogation of Art. 19 eIDAS as proposed in Art. 39 NIS 2 we might actually lower the level of security of these services. Therefore, **we are of the view that eIDAS should remain lex specialis to NIS 2 and the Art. 39 NIS 2 should be deleted**. We are concerned about both security measures and incident reporting specificities that might not be sufficiently covered by the NIS 2 framework.

Given the more general regulatory approach of eIDAS in relation the trust service providers, we are concerned that by a sole derogation of Art. 19 (or its equivalent in the revised eIDAS Regulation) by the NIS 2 **we might omit and lose certain non-cyber security aspect related to the trust service providers currently addressed by eIDAS Regulation**, such as physical identification of persons or procedures for issuing certificates.

Similarly, **the NIS 2 might not cover all types of incidents currently reported under eIDAS framework**. For instance, an information about a false statement that a private key has been stored in the QSCD (when it actually was not) or a notification about time stamps delays.

If, however, the NIS 2 security framework replaced the eIDAS security framework, we think that it would be of utmost importance to draft the revised eIDAS so as that we don't lose any security best practice addressed to trust service providers.

In addition, we would like to stress that the NIS 2 proposal does not reflect the difference between qualified and non-qualified trust service providers and includes both categories of the providers into the essential entities' category. We think that in case that the trust service providers were regulated by the NIS 2 the inclusion of non-qualified trust service providers into the essential entities' category should be reconsidered.

Lastly, we would like to highlight that if the Art. 19 (or its equivalent in the revised eIDAS Regulation) were repealed at the time of the NIS 2's entry into force, **we risk an 18 months' time gap of no-regulation security regime for trust service providers** during which they would not be obliged to take any security measures.

DORA

We believe that further clarification and adjustment of relation between NIS and DORA is necessary.

The incident handling for financial market EEs should remain with CSIRTs, as it has the necessary facilities and experience for incident handling, while building such facilities in the NCA would create unnecessary expenses as well as redundant duplication of CSIRTs. So, we propose to change the art. 17 of DORA.

In order for CSIRTs to be able to provide targeted help and adequate response, it is necessary that they have the knowledge of the particular ICT systems of the entity they are supposed to help. Therefore, transferring all the competence over ICT risk management supervision to financial NCAs without further involvement or assistance of NIS authorities would deteriorate the abilities of CSIRTs to provide adequate support in time of need. Therefore, we believe that it is necessary to facilitate appropriate cooperation of the NIS authorities and financial competent authorities in relation to ICT risk management supervision for financial entities identified as essential entities in the NIS II. Therefore So, we propose to change art. 42 of DORA.

Apart from the proposed enhanced cooperation for the purposes of exercise of supervisory tasks over the financial entities that are essential entities, there is also the need to share information between NCAs and NIS authorities that would allow NIS authorities and CSIRTs teams to fulfil their roles. Therefore, we also propose an amendment in Art. 49 para 3 related to the professional secrecy.

CER

General remark: *Given the fact that the WP PROCIV's deadline for draft changes request to the CER Directive has been set until 3th June 2021, the national coordination at national level is still taking place, the concerns expressed below shall therefore be considered as preliminary and non-exhaustive.*

Art. 2 (2) subparagraph 2 NIS 2
According to this Article, it is proposed that Member States shall established a list of entities pursuant to points -b) to g) and submit it to the Commission by **6 months** after the transposition deadline.
That list should be submitted to the Commission at the latest **2 years** after entry into force (transposition deadline 18 months + 6 months).

According to Art. 6 (2) CER Directive proposal, Member States shall submit to the Commission by **3 years and three months** after the entry into force the number of critical entities identified for each sector and subsector referred to in the Annex and the service/services referred to in Art. 4(1) that each entity provides.

Some essential entities (even not everyone) identified by NCAs at least according Art. 2/2 criteria d)-f) could therefore overlap with following identification of the essential entities as critical entities according to the CER Directive. **Even that NIS 2 does not intend to share the list of those "CER critical entities" with the Commission, in practice, some of those critical entities could be covered in that list based on their identification according to the previous letters.** This would be in contrary to abovementioned CER provision, which foresees to share only number of critical entities with the Commission, not their list. **Therefore, we insist on not submitting the list of entities according to the Art. 2 subparagraphs 2 letters d) through f) to the Commission.**

Art. 29 (9) NIS 2 – deletion
This provision seems to impose an additional burden on the NCAs according to the NIS2. Given the fact that both CER and NIS2 sets down framework both for the mutual information exchange and cross-border cooperation within their scope, this cooperation issue should already be covered within the framework for enhanced coordination (according rec. 14 and Art. 5/1 f)). Therefore, this paragraph should be deleted, or, at least transferred to the provisions regarding the mutual assistance (Art. 34) that also cover a possibility to refuse such assistance request in case of non-competence or non-proportionality.

GDPR

Recital 59

We strongly suggest amending the last sentence as follows: "Where processing includes personal data such processing shall strictly comply with Union data protection law, **with due regard to Article 5 paragraph 1 of the GDPR."**

We believe that it would be beneficial to add this reference so to underline the importance of key principals relating to processing of personal data.

Recital 69

We think that "legitimate interest" is not a suitable legal basis for the processing of personal data in the NIS 2 context. We suggest using "public interest" legal basis instead.

CSA

A new task for ENISA regarding assessing (and creating) cybersecurity index as referred to in Article 15 (which is assessed in a biennial report on the state of cybersecurity) is not reflected within the provisions of Regulation 2019/881 (Cybersecurity Act). Therefore NIS 2 should also include **appropriate amendment of Regulation 2019/881 in that regard.**

DENMARK

Danish drafting proposal on the interaction between the NIS2 Directive and relevant sectoral legislation listed hereunder:

Recitals:

13b) Commission Implementing Regulation (EU) 2019/1583 and Commission Regulation (EU) XXXX/XXXX** should be considered to be a sector-specific Union legal act in relation to this Directive with regard to the civil aviation sector organisations. The provisions of Implementing Regulation (EU) 2019/1583* and Regulation (EU) XXXX/XXXX** relating to identifying and protecting the critical information and communications technology systems and data from cyber-attacks and information security risks, the management of information security risks and reporting of incidents should apply instead of those set up under this Directive, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations and supervision to any civil aviation organisations covered by Implementing Regulation (EU) 2019/1583* and Regulation (EU) XXXX/XXXX**, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive.*

** Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures*
*** Commission Regulation (EU) XXXX/XXXX of XX Month 202X on the introduction of organisation and authority requirements for the management of information security risks related to information systems used in civil aviation.*

ESTONIA

	Commission proposal	EE amendment
All sectorial acts:	**Recital 12***: […] Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply.[…]*	*[…] Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply.* ***Those sector-specific legal acts should ensure that the minimum threshold for security measures and incident reporting laid out in this horizontal Directive, is met.[…]*** *(**explanation:** it should be highlighted to a greater degree that the NIS directive is the pivotal EU legal act in the sphere of cybersecurity, which sets the baseline for cybersecurity measures for every sector concerned)*
DORA Regulation	**Recital 13:** […] Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX.[…]	**Recital 13:** […] Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered **on an at least equal level** by Regulation XXXX/XXXX.[…]
eIDAS Regulation	**Article 39**: *Amendment of Regulation (EU) No 910/2014* *Article 19 of Regulation (EU) No 910/2014 is*	***Deletion of the article*** *(**explanation**: involvement of trust service providers (TSP) under the NIS 2.0 needs further analysis; our*

	deleted.	*prevailing position is that the consequential disadvantages outweigh the advantages in what concerns bringing TSP-s under the NIS 2.0)*
CER Directive	- **Article 18**	- **Article 18 (new paragraph 3)** : ***Member States shall ensure that, where considering appropriate measures referred to in point (a) of paragraph 2, entities from the digital infrastructures sector shall take into account relevant elements of physical security.*** *(**explanation** : Recital 14 of the CER : "Entities pertaining to the digital infrastructure sector are in essence based on network and information systems and fall within the scope of the NIS 2 Directive, which addresses the physical security of such systems as part of their cybersecurity risk management and reporting obligations." Reading the current NIS 2.0 proposal and the article 19, there is no reference to physical security nor can we assume that the risk assessments (although here we use the term "risk analysis") that ought to be undertaken by entities will be executed on a level comparable to the CER directive.*
	Recital 14: *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)*	Recital 14: *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.	*XXX/XXX in the context of information sharing on incidents, cyber **and non-cyber** threats, **enhancing resilience** and the exercise of supervisory tasks.* *(**explanation**: Commission's proposals entail a one-way information flow, from NIS CA's to CER CA's. Receiving overviews on physical threats helps the NIS CA's to draw a better picture of the threat landscape and will create reciprocity in the cooperation between authorities.*

FINLAND

Disclaimer: *Please note, that the following comments are not exhaustive and might be elaborated further.*

eIDAS and NIS 2 alignment

General observation

In the area of Trust Services, a customized supervisory system has been established by eIDAS regulation which, among other things, already covers all the essential aspects of NIS directive, so it is highly important not to jeopardise trust services market and maintain the current system due to its superior level of maturity and harmonisation level.

If there is an intention to include Trust Services into scope of NIS directive, we propose to do that in the same way as it is done with financial sector (*leaving eIDAS regulation as lex specialis with its Article 19)* and additionally define within NIS how eIDAS supervisory bodies will cooperate with NIS supervisory bodies. *[Relevant parts of NIS directive: Cooperation - Preamble (14), Article 11 (4), Article 12(3); Notification of incidents – Preamble (23)]*.

Specific comments:

Should NIS supervisory body be involved in the process of granting/withdrawing qualified status?

In our opinion NIS supervisory body should not be involved in this process directly, because having two supervisory bodies would be additional and unnecessary burden to trust service providers and would jeopardise trust services market.

The best-case scenario would be just explicitly defining how eIDAS supervisory bodies cooperate with NIS supervisory bodies by giving possibility for eIDAS supervisory bodies to get opinion/consultation from NIS supervisory body *(in case there would be such need before making decision whether to grant/withdraw qualified status to trust service provider)*.

How eIDAS supervisory body could get information about incidents?

The best-case scenario would be following the approach of financial sector – incidents could be notified to eIDAS supervisory body (*like it is done now)* and eIDAS supervisory body would then immediately share significant incidents with NIS supervisory body.

Alternative approach could be defining within EU legislation *(to have harmonised approach all over EU)* that significant incidents in the area of trust services should be notified to NIS supervisory bodies, and then these bodies should immediately share these incidents eIDAS supervisory bodies.

How to deal with the issue of different scopes of eIDAS regulation *(security to Trust services overall)* and NIS directive *(only security of Network and Information systems of the provider)?*

The best and easiest option would be choosing the same approach as it is foreseen with financial sector and keep Article 19 within eIDAS regulation.

Alternative option would be to amend Article 19 of eIDAS regulation and leave there all the aspect that will not be covered by NIS directive. Detailed analysis of both documents should be done in order to assess whether this approach is feasible.

How to deal with the issue tight relation of Article 19 and other article of eIDAS regulation*?*

The best and easiest option would be choosing the same approach as it is foreseen with financial sector and keep Article 19 within eIDAS regulation.

Not sure whether there is a simple alternative solution. To assess whether and how it would be possible to avoid such issues, detailed analysis of eIDAS regulation should be performed.

One of the issues for example would be Liability of Trust service provider (Article 13) – if Article 19 would be removed, Trust Service providers would not be liable for their services in case of issues with Network and Information systems, because Article 13 defines liability only in case of failure to comply with the obligations under the eIDAS Regulation *(if Article 19 will be removed – these requirements will not be a part of eIDAS anymore and this will dramatically lower liability of trust service providers)*.

How to deal with the issue that Network and information security requirements will not be included within conformity assessment reports?

The best option would be choosing the same approach as it is foreseen with financial sector and keep Article 19 within eIDAS regulation.

Alternative option would be defining the scope of conformity assessment reports and explicitly requiring that they would include security of Network and Information systems aspects. Of course, it would be quite difficult to do as this would require amendment of eIDAS regulation (not sure whether that could be done with directive).

How not to decrease the level of harmonisation?

All above aspects should be explicitly defined within EU documents and not left for the national legislation.

EECC and NIS 2 alignment

General observation:
We are still cautious about the removal of Articles 40 and 41 from EECC.

Specific comments:

Regarding recital 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[22] and Directive (EU) 2018/1972 of the European Parliament and of the Council[23] related to the imposition of security and notification requirement on these types of entities should ~~therefore be repealed~~ **complement 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[24].

Regarding 11.4 Article:
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 authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]**, national regulatory authorities designated in accordance with Directive (EU) 2018/1972** and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39][the DORA Regulation] within that Member State.

Accordingly, we would also suggest the deletion of **Article 40** from NIS 2 proposal, which currently aims to delete Articles 40 and 41 from EECC.

GDPR and NIS 2 alignment

General observation:
NIS 2 Proposal refers to Regulation (EU) 2016/679 but its specific timelines for notification of the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation are not transferred.

Specific comments:
For that reason, for **Article 32.1**, we would suggest:

Instead of using terminology "*within a reasonable time*", use "*without undue delay and, where feasable, not later than 72 hours after becoming aware of it*".

DORA and NIS 2 alignment

General observation:

Definitions in both these documents should be aligned. Currently there is a discrepency between the two documents, e.g. NIS 2 uses "*incident*" and, most importantly, when it comes to reporting obligations "*significant incident*" (Article 20.3); whereas DORA currently uses "*ICT related incidents*" (Articles 15 and 16) and "*major ICT-related incidents*" (Article 17).

Article 2.6 and recitals 12 and 13:

NIS 2 text clearly states the intention of financial sector to be considered as *lex specialis*, justifying that in such case, the sector-specific requirements should be "*of at least an equivalent effect to the obligations laid down in this Directive*". However, differently from NIS 2, there is currently no requirement in DORA for financial entities to report significant threats. Seeking for NIS 2 to maintain a horizontal baseline when it comes to cybersecurity requirements, regardless of a given sector, our suggestion would be to include the reporting obligation for significant cyber threats for financial entities in DORA.

CER and NIS 2 alignment:

Specific comments (Article 29.9):

Currently the cooperation between NIS 2 and CER competent authorities is not clear. Understanding that all critical and equivalent to critical entities are within the scope of NIS 2 (except for financial sector, which would have a *lex specialis status*), NIS 2 competent authorities should, in the same vein, exercise their supervisory and enforcement powers. Understandibly, in such situations NIS 2 authorities should inform CER competent authorities but the supervisory and enforcement powers of NIS 2 competent authorities should not be conditional upon request from CER competent authorities (as currently Article 29.9 suggests). Therefore, the following sentence should be deleted: "*Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent*." Instead, the following sentence could be added: "*Competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] may also request the competent authorities under this Directive to exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent*."

FRANCE

Dans la perspective de la réunion du groupe horizontal sur les questions cyber du 18 mai 2021, les autorités françaises souhaitent partager avec la Présidence des propositions d'amendements portant sur les liens entre les différents actes européens et le projet de directive relative aux mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union (NIS2).

Les autorités françaises remercient la Présidence pour la lecture initiale du projet de révision de la directive NIS et souligne toute la pertinence de l'approche choisie : les discussions sur les interactions entre le projet de directive et les actes sectoriels sont tout à fait dimensionnantes pour la poursuite des négociations, en permettant notamment de traiter de manière transverse l'extension du périmètre de NIS. À cet égard, les autorités françaises saluent l'approche ambitieuse proposée par la Commission européenne, l'extension du périmètre devant répondre à l'état de la menace. Les autorités françaises tiennent toutefois à proposer plusieurs ajustements, afin d'assurer la bonne articulation de la directive NIS avec plusieurs actes européens.

[RGPD] Au **considérant 69**, les autorités françaises soulignent que, compte tenu de la volonté de la Commission d'aligner la proposition de directive avec le règlement (UE) 2016/679 du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, il conviendrait de garantir que les activités nécessitant le traitement de données personnelles menées par les autorités compétentes pour NIS, au titre de la sécurité nationale, soient préservées. Si la directive exclut de son périmètre les compétences des États membres en matière de sécurité nationale (article 2 paragraphe 3), il convient de garantir ces compétences (audits, tests de pénétration, détection, etc.), intrinsèquement dépendantes du traitement de données personnelles. Les autorités françaises souhaitent donc introduire une référence à l'article 23 du règlement (UE) 2016/679 qui prend en considération cette dimension opérationnelle :

> *"The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679* ***or a necessary and proportionate measure to safeguard national security in compliance with the article 23 of the aforementioned Regulation.*** *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 types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.*"

[CECE] L'extension de la directive NIS aux opérateurs de télécommunications ne doit en aucun cas affaiblir le cadre juridique régulant ces opérateurs. A défaut de conserver les articles 40 et 41 du Code européen des communications électroniques (CECE), il est indispensable d'en préserver le périmètre au sein de la directive NIS, en reflétant *in extenso* le périmètre compris aux articles 40 et 41 de la directive (UE) 2018/1972 par l'introduction de la notion de « services » aux articles suivants :

- à l'**article 4 paragraphe 2**, afin de garantir les obligations pesant sur les opérateurs de se prémunir de pannes non-cyber sur leurs services :

*"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 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, **services** and information systems";*

- à l'**article 18 paragraphe (1)**, afin de conserver les obligations pesant sur les opérateurs de prendre « des mesures techniques et organisationnelles adéquates et proportionnées pour gérer les risques en matière de sécurité des réseaux et des services de manière appropriée » qui permettront de ne pas créer de vide juridique en la matière entre le CECE et NIS2. Par ailleurs, l'article 40 proposant le recours à des mesures concernant le chiffrement, il pourrait être proposé la reprise *in extenso* dans NIS2 de :

*"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 and information systems appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services";*

- par conséquent, les autorités françaises seront vigilantes afin que l'esprit des mesures prévues au titre de l'article 41 de la directive (UE) 2018/1972 soit préservé à **l'article 29** du projet de directive NIS2.

[eIDAS] Les autorités françaises, au même titre que de nombreux États membres, ont partagé leurs doutes sur le fait que l'inclusion des prestataires de services de confiance non qualifiés dans le périmètre de la directive NIS soit conforme au principe de proportionnalité. Ainsi, une étude d'impact approfondie et affinée de la part de la Commission européenne permettrait d'éclairer les discussions au sein du Conseil et de s'assurer que ces dispositions ne déstructureraient pas le secteur.

Dans l'attente d'une telle analyse, les autorités françaises proposent de n'inclure que les prestataires de confiance qualifiés dans le périmètre de la directive NIS2 et proposent à cette fin les ajustements suivants :

- à l'**article 2**, la suppression du paragraphe 2 (a) (ii) *"trust service providers referred to point 8 of Annex I*" ;
- à l'**Annexe I** *: "8. Digital infrastructure - Trust service providers referred to ~~in point (19)~~ **in point (20)** of Article 3 of Regulation (EU) No 910/2014*";
- à l'**article 4**, l'introduction en miroir de l'Annexe I, de la définition des prestataires de confiance de services qualifiés :

"Qualified trust service provider" means a qualified trust service provider within the meaning of article 3 (2) of regulation No 910/2014.

Par ailleurs, l'extension du périmètre de la directive NIS doit permettre l'essor du marché des prestataires de services de confiance. Ainsi, à l'**article 21 paragraphe** 1, les autorités françaises proposent d'ajouter les services de confiance qualifiés et les schémas d'identification électronique notifiés en vertu du règlement (UE) 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, comme moyen de répondre aux exigences de la directive NIS.

"In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to ***use qualified trust services or notified electronic identification schemes under the terms of Regulation n°910/2014,*** *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*".

[*Lex specialis*] Les autorités françaises rappellent leurs préoccupations de voir les initiatives sectorielles - à l'instar du projet de règlement sur la résilience opérationnelle numérique (DORA) notamment, mais également des mesures prises dans le secteur du secteur aérien à l'image du règlement (UE) 2015/1998 relatif à la sûreté du transport aérien - venir fragmenter le cadre réglementaire européen en matière de cybersécurité.

Les autorités françaises soulignent l'importance de garantir au mieux que la directive NIS demeure le cadre législatif horizontal de référence et que les éventuelles initiatives sectorielles s'appuient sur le socle de base d'exigences existant en matière de cyber sécurité. Cela est d'autant plus important qu'il importe de ne pas faire peser des orientations contradictoires sur les secteurs amenés à investir dans le renforcement de leurs capacités.

Afin de garantir que NIS demeure le cadre de référence, les autorités françaises proposent, au **considérant 12**, les modifications suivantes :

"(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply.

(12bis) At the same time, such sector-specific legislation and instruments should not add extra-burden to both providers of certified ICT products, services and processes and trusted providers of cybersecurity services such as security audit or incident response. In order to avoid conflicting risk management and incident notification requirements stemming from sector-specific legislation and instruments, the Commission ~~*may*~~ ***should*** issue guidelines in relation to the implementation of the lex specialis ***taking relevant opinions, guidelines and best practices of the NIS Cooperation Group into account***.

(12ter) 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."

À **l'article 2**, les autorités françaises proposent d'ajouter en conséquence un nouveau paragraphe :

*"****(7new). In order to ensure that sector-specific legislation and instruments meet the minimum security requirements laid down by the Directive, the Commission shall issue guidelines in relation to the implementation of the lex specialis taking opinions, guidelines and best practices of the NIS Cooperation Group into account.***

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

automatic and direct forwarding of the notifications to the national competent authority or the CSIRT under this Directive by the authority that receives incident notifications under the sector-specific act."

De même, à **l'article 12**, les autorités françaises suggèrent également d'adapter le paragraphe 4, en ajoutant une nouvelle tâche au groupe de coopération NIS :

> "***(12 bis) providing advice and cooperating with the Commission on draft Commission guidelines in relation to the implementation of the lex specialis;***"

[DORA] Aux **considérants 13 et 23**, les autorités françaises proposent la modification ci-après, afin de rendre immédiate et automatique la transmission des informations :

> "*(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 and reporting obligations~~, information sharing~~ and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows all financial supervisors, the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX, to participate in 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* ***make sure the competent authorities of this directive or the CSIRT receive automatic and immediate acces to all ICT-related incident notification*** *~~transmit details of major ICT related incidents 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.*
>
> *(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. 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 incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should ~~be able to~~ forward~~, as appropriate,~~* ***immediately and automatically*** *to the relevant national competent authorities or CSIRTs under this Directive.*"

[REC] Afin d'assurer une meilleure coordination entre les projets de directive, les autorités françaises souhaitent introduire une modification au **considérant 14,**permettant de bien prendre en compte l'ensemble du spectre couvert par ces deux directives :

"(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 17 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 as well as on the cybersecurity, ***resilience and physical security*** *measures taken by* ~~*critical*~~ ***essential*** *entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose."*

Les autorités françaises se tiennent à la disposition de la Présidence pour toute précision utile.

GERMANY

Change requests and drafting proposals by Germany

Preliminary note: During the HWPCI meeting of 28 April 2021, the chair announced a general discussion on the interplay of NIS2 with other legislative acts and proposals (i.e. draft DORA directive, draft CER regulation, eIDAS regulation, EECC directive and GDPR) for the HWPCI meeting on 5 May 2021 and invited Member States to present their respective change requests and drafting proposals until 14 May 2021. This document contains the current change requests and drafting proposals by Germany until that time.

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
1.	(*lex specialis*)	Recital 12	• The first change is of an editorial nature. • The reasoning for the addition is as follows: If the scope of a sector-specific act and NIS2 in a certain sector overlap, but the sector-specific act does not cover all entities in that sector covered by NIS2, the *lex specialis* provision should only apply to those entities under the scope of the sector-specific act. • Therefore, those entities in that sector not being covered by that sector-specific act should continue to be covered by NIS2. • This is a necessary precaution to prevent a decrease in the level of cybersecurity through potential regulatory gaps.	*Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector-specific Union legal act requires essential or important entities to adopt* ***measures of at least an equivalent effect to the obligations laid down in this Directive, pertaining in particular to*** *cybersecurity risk management measures* ~~*or to notify*~~ ***and notification of*** *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.* ***However, if a sector-specific legislation does not cover at***

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
				least all entities in a specific sector also covered by this directive, the provisions of this directive should continue to apply to those entities not covered by the sector specific legislation.*The Commission may issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.*
2.	DORA	Recital 13	• In order to enable NIS2 competent authorities to carry out the tasks laid out in this directive, it is crucial that the authorities have immediate access to all relevant information concerning cybersecurity threats and incidents. • According to Art. 2 para. 6 only the provisions of this directive on cybersecurity risk management measures and notification requirements, including the provision on supervision and enforcement laid down in Chapter VI, should not apply. Therefore, the provisions of this directive on information	*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*

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
			sharing should continue to apply.	*should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations~~,~~ ~~information sharing~~ and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows all financial supervisors, the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX, to participate in 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* ***make sure the competent authorities of this directive receive automatic and immediate access to all ICT-related incident notifications*** ~~*transmit details of major ICT-related incidents also to the single points of contact designated under this Directive*~~*.* ***This can be achieved by, for example, automatic and direct forwarding of incident notifications or a common reporting platform.*** *Moreover,*

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
				Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.
3.	CER	Recital 14	• Since a majority of entities will be covered by both the NIS2 directive and the CER directive, competent authorities under both directives should exert their best effort in order to align supervisory activities and incident notification processes under both directives.	*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 as well as on the cybersecurity measures taken by critical entities.* ***Furthermore, in order to streamline***

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
				supervisory activities between the competent authorities of both directives and in order to minimize the administrative burden for the entitites, authorities under both directives should align incident notification templates and supervisory processes as best as possible. *Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.*
4.	GDPR	Recital 14a (new)	• In order to ensure coherence between this Directive and the existing EU legislation on data protection, especially the General Data Protection Regulation (GDPR) and the ePrivacy Directive, and to prevent legal uncertainty it has to be clarified that o this Directive is without prejudice inter alia to the competences of the Independent Data Protection authorities to enforce the GDPR in cases of personal data breaches as well as the obligation for the controller to report those breaches to these	***(14a) This Directive does not seek to affect the application of Union law on the processing of personal data, especially Regulation (EU) 2016/679 and Directive 2002/58/EC, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments. To any processing of personal data falling within the scope of this Directive, Union law on the protection of personal data and privacy shall apply.***

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
			authorities without undue delay, and o all processing of personal data within the scope of this Directive must comply with the requirements of the Union's data protection legislation. • We suggest that this be laid down in Article 2 and, in addition, in a recital (however, the location we are proposing here for the recital is a first approach and might need further examination). • These proposals are also in line with suggestions of the EDPS (see EDPS Opinion - ST 7151/20 – 11.03.2021, paragraphs 27-31.)	
5.	DORA	Recital 23	• Immediate and automatic forwarding of information is crucial in our view.	*Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. 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 incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should ~~be able to~~ forward~~, as~~*

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
				~~*appropriate,*~~ ***immediately and automatically*** *to the relevant national competent authorities or CSIRTs under this Directive.*
6.	GDPR	Article 2 para. 3a (new)	• See no. 4 above.	***(3a) Union law on the protection of personal data shall apply 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.***
7.	(*lex specialis*)	Article 2 para. 6	• The *lex specialis*-clause in article 2 para. 6 NIS2, should be clarified that in case of sector-specific acts, the obligations under NIS2 do not apply only to those important and essential entities that are within the scope of the sector-specific act and not to the entire sector across-the-board. Otherwise, this could lead to setbacks in the progress already achieved.	*Where provisions of sector-specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply* ***to such essential or important entities****.*
8.	(*lex specialis*)	Article 2 para. 7 (new)	• In its current form, the *lex specialis*-clause will – in our view – foster regulatory fragmentation, double regulation and eventually lead to conflicting obligations for entities.	***In order to safeguard a coherent minimum standard of cybersecurity across all sectors , sector-specific acts referred to in paragraph 6 should include*** ***(a) cybersecurity risk management***

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
			• Already existing sector-specific acts may encourage legislative initiatives in other sectors to create sector-specific cybersecurity measures and incident notifications as well. While sector-specific acts may be tailored to those sector's specific needs, they should not lead to a decline of the cybersecurity level defined by the cybersecurity measures and incident notifications defined by NIS2. • NIS2 should not limit the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications, as rightly stated in its recital 12. • But we believe it is important to prevent regulatory fragmentation in the best way possible. The horizontal nature of NIS2 should not only be emphasized in the recitals but also in the articles. • Therefore, as a sort of blueprint for future legislative initiatives NIS2 needs to (a) contain a minimum set of cybersecurity measures as a sort of baseline and (b) provide guidelines for immediate receipt of the notifications by the NIS2 national competent authority. The latter goal can be achieved in two ways – either by (i) granting access to the notifications, or (ii) forwarding of these	***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 incidents or significant cyber threats that are at a minimum equivalent to those laid down in article 20 paragraphs 1 through 4 and further include:*** ***(i) automatic and direct access to the incident notifications by the national competent authority under this Directive through a common reporting mechanism; or*** ***(ii) automatic and direct forwarding of the notifications to the national competent authority under this Directive by the authority that receives incident notifications under the sector-specific act.***

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
			notifications.	
9.	CER	Article 11 para. 5	• This is a one-sided obligation that needs to be balanced between the NIS2-NCA and the CER-NCA.	*Member States shall ensure that their competent authorities* ***and the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]*** *regularly* ~~*provide*~~ ***exchange*** *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.*
10.	CER	Article 29 para. 9	• This obligation appears superfluous and should be deleted. The information exchange between the NIS2-NCA of different MS is regulated in NIS2, that between the CER-NCA of different member states is regulated in CER. Moreover, both NIS2 and CER regulate the information exchange between the NIS2-NCA and the CER-NCA of a given member state. The additional obligation of the NIS-2NCA to inform the CER-NCA of a different MS pursuant to Art. 29	~~*Member States shall ensure that their competent authorities inform the relevant competent authorities of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical*~~

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
			para. 9 NIS2 appears therefore to be superfluous while imposing an unnecessary additional burden.	~~*Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.*~~
11.	eIDAS	Article 39	• As the Commission has – as of now – not presented its proposal for an eIDAS review, the following change request is based on NIS2 only and may possibly change after the complete proposal for a revised framework for trust service providers has been released. • We propose the deletion of article 39 NIS2. • If article 39 would remain, this would lead to the deletion of article 19 eIDAS and thus the inclusion of trust service providers as essential entities in NIS2. In our view, this will – lead to a lowering of the current level of security, as some relevant security aspects currently monitored or foreseen under eIDAS would not fall within the scope of NIS2 or would not be appropriately covered by it (e.g.	~~*Article 19 of Regulation (EU) No 910/2014 is deleted.*~~

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
			NIS2 does not provide for notification of private parties concerned and does not provide references to the latest technological developments, but only state of the art); – lead to greater fragmentation instead of harmonization. Currently, eIDAS as a regulation uniformly regulates the security requirements for trust service providers in Europe. Replacing this Europe-wide uniform requirement with a directive will lead to inconsistencies and confusion, as the directive may be implemented differently in each country; – lead to a loss of knowledge and long-standing competencies due to the takeover of a functioning system by another competent authority. • As part of the eIDAS evaluation, the Commission itself determined that rules governing trust service providers, in particular, do not require significant changes because the current system is working smoothly. If the regulatory framework for trust service providers needs to be adapted to security	

No.	Legislative act / proposal	NIS2 reference	Change request	Drafting proposal
			requirements of NIS2, this can be done within the framework of the Commission proposal for eIDAS review. • To ensure continuity and since the security mechanisms for trust service providers have been functioning and matured for 20 years, we strongly advocate keeping trust service providers – as is currently the case – within eIDAS as *lex specialis* to NIS2.	

IRELAND

EECC

EECC has proven to be a good framework to address the security threats posed to electronic communications sector. In our view, the security aspects of electronic communications sector are highly specific, complex and form part of a wider regulatory EECC framework which by a sole derogation of Art. 40 and 41 EECC would erode. While we acknowledge that the security of electronic communications sector is of great interest of NIS authorities and they should participate in enhancing the cybersecurity practices of electronic communications sector entities, we think that **the basis for (not only cyber) security-related obligations addressed to electronic communications sector should remain in Art. 40 and 41 EECC** and the primary responsibility for ensuring high level of security of electronic communications sector entities should continue to lie with EECC authorities which shall closely cooperate with the NIS authorities.

In practice, the security measures under EECC comprise of measures aimed at protection of networks against disruptions caused by electromagnetic interference and processing loading or measures aimed at protection of interoperability of services. All of these are non-cyber measures would remain unaddressed if the Art. 40 and 41 were solely derogated. Furthermore, our EECC authority deals, on a daily basis, with incidents caused by human errors during the operation of equipment or facilities, system failures, natural phenomena or of similar nature. Such incidents represent a majority of incidents reported by electronic communications sector entities to our EECC authority. We believe that there is not much of an added value in notifying CSIRTs or NIS authorities about such incidents. As a matter of fact, given the large number of entities from electronic communications sector, administrating such types of incidents would be a considerable additional burden for CSIRTs operation.

If the Art. 40 and 41 were derogated, it would be necessary to ensure that non-cyber risks are duly addressed in the EECC framework. In addition, we would suggest reconsidering inclusion of number-independent interpersonal communication services into the essential entities' category.

eIDAS

In general, we think that the current regulatory regime related to the security of trust service providers in eIDAS is well-functioning and by the sole derogation of Art. 19 eIDAS as proposed in Art. 39 NIS 2 we might actually lower the level of security of these services. Therefore, **we are of the view that eIDAS should remain lex specialis to NIS 2 and the Art. 39 NIS 2 should be deleted**. We are concerned about both security measures and incident reporting specificities that might not be sufficiently covered by the NIS 2 framework.

Given the more general regulatory approach of eIDAS in relation the trust service providers, we are concerned that by a sole derogation of Art. 19 (or its equivalent in the revised eIDAS Regulation) by the NIS 2 **we might omit and lose certain non-cyber security aspect related to the trust service providers currently addressed by eIDAS Regulation**, such as physical identification of persons or procedures for issuing certificates.

Similarly, **the NIS 2 might not cover all types of incidents currently reported under eIDAS framework**. For instance, an information about a false statement that a private key has been stored in the QSCD (when it actually was not) or a notification about time stamps delays.

If, however, the NIS 2 security framework replaced the eIDAS security framework, we think that it would be of utmost importance to draft the revised eIDAS so as that we don't lose any security best practice addressed to trust service providers.

In addition, we would like to stress that the NIS 2 proposal does not reflect the difference between qualified and non-qualified trust service providers and includes both categories of the providers into the essential entities' category. We think that in case that the trust service providers were regulated by the NIS 2 the inclusion of non-qualified trust service providers into the essential entities' category should be reconsidered.

Lastly, we would like to highlight that if the Art. 19 (or its equivalent in the revised eIDAS Regulation) were repealed at the time of the NIS 2's entry into force, **we risk an 18 months' time gap of no-regulation security regime for trust service providers** during which they would not be obliged to take any security measures.

DORA

We believe that further clarification and adjustment of relation between NIS and DORA is necessary.

The incident handling for financial market EEs should remain with CSIRTs, as it has the necessary facilities and experience for incident handling, while building such facilities in the NCA would create unnecessary expenses as well as redundant duplication of CSIRTs. So, we propose to change the art. 17 of DORA.

In order for CSIRTs to be able to provide targeted help and adequate response, it is necessary that they have the knowledge of the particular ICT systems of the entity they are supposed to help. Therefore, transferring all the competence over ICT risk management supervision to financial NCAs without further involvement or assistance of NIS authorities would deteriorate the abilities of CSIRTs to provide adequate support in time of need. Therefore, we believe that it is necessary to facilitate appropriate cooperation of the NIS authorities and financial competent authorities in relation to ICT risk management supervision for financial entities identified as essential entities in the NIS II. Therefore So, we propose to change art. 42 of DORA.

Apart from the proposed enhanced cooperation for the purposes of exercise of supervisory tasks over the financial entities that are essential entities, there is also the need to share information between NCAs and NIS authorities that would allow NIS authorities and CSIRTs teams to fulfil their roles. Therefore, we also propose an amendment in Art. 49 para 3 related to the professional secrecy.

CER

General remark: *Given the fact that the WP PROCIV's deadline for draft changes request to the CER Directive has been set until 3th June 2021, the national coordination at national level is still taking place, the concerns expressed below shall therefore be considered as preliminary and non-exhaustive.*

Art. 2 (2) subparagraph 2 NIS 2
According to this Article, it is proposed that Member States shall established a list of entities pursuant to points -b) to g) and submit it to the Commission by **6 months** after the transposition deadline.
That list should be submitted to the Commission at the latest **2 years** after entry into force (transposition deadline 18 months + 6 months).

According to Art. 6 (2) CER Directive proposal, Member States shall submit to the Commission by **3 years and three months** after the entry into force the number of critical entities identified for each sector and subsector referred to in the Annex and the service/services referred to in Art. 4(1) that each entity provides.

Some essential entities (even not everyone) identified by NCAs at least according Art. 2/2 criteria d)-f) could therefore overlap with following identification of the essential entities as critical entities according to the CER Directive. **Even that NIS 2 does not intend to share the list of those "CER critical entities" with the Commission, in practice, some of those critical entities could be covered in that list based on their identification according to the previous letters.** This would be in contrary to abovementioned CER provision, which foresees to share only number of critical entities with the Commission, not their list. **Therefore, we insist on not submitting the list of entities according to the Art. 2 subparagraphs 2 letters d) through f) to the Commission.**

Art. 29 (9) NIS 2 – deletion
This provision seems to impose an additional burden on the NCAs according to the NIS2. Given the fact that both CER and NIS2 sets down framework both for the mutual information exchange and cross-border cooperation within their scope, this cooperation issue should already be covered within the framework for enhanced coordination (according rec. 14 and Art. 5/1 f)). Therefore, this paragraph should be deleted, or, at least transferred to the provisions regarding the mutual assistance (Art. 34) that also cover a possibility to refuse such assistance request in case of non-competence or non-proportionality.

GDPR

Recital 59

We strongly suggest amending the last sentence as follows: "Where processing includes personal data such processing shall strictly comply with Union data protection law, **with due regard to Article 5 paragraph 1 of the GDPR."**

We believe that it would be beneficial to add this reference so to underline the importance of key principals relating to processing of personal data.

Recital 69

We think that "legitimate interest" is not a suitable legal basis for the processing of personal data in the NIS 2 context. We suggest using "public interest" legal basis instead.

CSA

A new task for ENISA regarding assessing (and creating) cybersecurity index as referred to in Article 15 (which is assessed in a biennial report on the state of cybersecurity) is not reflected within the provisions of Regulation 2019/881 (Cybersecurity Act). Therefore NIS 2 should also include **appropriate amendment of Regulation 2019/881 in that regard.**

ITALY

"General Observations on the interaction between Directive NIS 2 and Sectoral Legislation"

General Considerations

- Recital: (12)
- Article 2/6

It seems important to avoid any confusion/uncertainty with respect to the applicable obligations/measures established, from one side, by the NIS 2 Directive and, from the other, by sectoral legislation. If not further specified, the notion of "equivalence" seems not sufficient to provide clear guidance to entities on the applicable law. Indeed, it leaves unresolved the issues to determine "who" defines the notion of equivalence, and according to "which" pre-established, clear and agreed criteria.

Furthermore, it seems relevant to better clarify the relationship between the NIS 2 Directive and other sectoral legal instruments concerning "safety aspects" related to the provision of services in specific sectors (e.g. aviation or energy).

DORA Regulation

- Recitals: (13), (23)
- Articles: 11/4, 12/3, 12/8

In light of the concerned recitals and provisions, the relationship between NIS 2 Directive and DORA Regulation could be better spelled out, with the aim to provide more clarity and legal certainty, for example, with regard to incident notification requirements. For the sake of clarity, it could help to explicitly mention which are the NIS 2 provisions that – consistently with Recital (13) of NIS 2 Directive –should not be applied in favour of DORA and/or vice versa. Moreover, it may help to better specify what is meant for "financial sector". DORA regulation has in scope, on the one hand, financial entities (clearly part of the financial sector *strictu sensu*); on the other hand, the ICT Third-Party Service Provider (given the services they provide to financial entities).

In addition, the DORA Regulation does not include national CSIRTs among the primary recipients of incident notifications together with DORA competent authorities. Given that recital (56) of the NIS 2 Directive states that Member States should establish a single entry point for all notifications required under NIS 2 Directive and also under other Union law, and also given the primary role of national CSIRTs under the NIS 2 Directive regarding incident notifications, shouldn't these latter have the same role under DORA, in order to maximize their early warning capabilities?

CER Directive

- Recitals: (14)
- Articles: 2/2/g, 5/1/f, 11/4, 11/5, 20/10, 29/9

Given that the coordination between NIS and CER competent authorities should be mutual, it seems important to ensure that information sharing – on, at least, incidents, threats, risks, and measures – between these authorities also include information on non-cyber risks and resilience, covered by the CER Directive.

GDPR

- Recitals: 25, 48, 56, 69, 77
- Articles: 26/1, 32/1, 32/2, 32/3

In light of recital (56), it seems important to provide for clear and effective harmonisation between obligations on incidents reporting, especially when an incident also entails a personal data breach to be reported – according to the GDPR – to National Data Protection Authorities.

LITHUANIA

Disclaimer: *Please note, that the following comments are not exhaustive and might be elaborated further.*

eIDAS and NIS 2 alignment

General observation

In the area of Trust Services, a customized supervisory system has been established by eIDAS regulation which, among other things, already covers all the essential aspects of NIS directive, so it is highly important not to jeopardise trust services market and maintain the current system due to its superior level of maturity and harmonisation level.

If there is an intention to include Trust Services into scope of NIS directive, we propose to do that in the same way as it is done with financial sector (*leaving eIDAS regulation as lex specialis with its Article 19)* and additionally define within NIS how eIDAS supervisory bodies will cooperate with NIS supervisory bodies. *[Relevant parts of NIS directive: Cooperation - Preamble (14), Article 11 (4), Article 12(3); Notification of incidents – Preamble (23)]*.

Specific comments:

Should NIS supervisory body be involved in the process of granting/withdrawing qualified status?

In our opinion NIS supervisory body should not be involved in this process directly, because having two supervisory bodies would be additional and unnecessary burden to trust service providers and would jeopardise trust services market.

The best-case scenario would be just explicitly defining how eIDAS supervisory bodies cooperate with NIS supervisory bodies by giving possibility for eIDAS supervisory bodies to get opinion/consultation from NIS supervisory body *(in case there would be such need before making decision whether to grant/withdraw qualified status to trust service provider)*.

How eIDAS supervisory body could get information about incidents?

The best-case scenario would be following the approach of financial sector – incidents could be notified to eIDAS supervisory body (*like it is done now)* and eIDAS supervisory body would then immediately share significant incidents with NIS supervisory body.

Alternative approach could be defining within EU legislation *(to have harmonised approach all over EU)* that significant incidents in the area of trust services should be notified to NIS supervisory bodies, and then these bodies should immediately share these incidents eIDAS supervisory bodies.

How to deal with the issue of different scopes of eIDAS regulation *(security to Trust services overall)* and NIS directive *(only security of Network and Information systems of the provider)?*

The best and easiest option would be choosing the same approach as it is foreseen with financial sector and keep Article 19 within eIDAS regulation.

Alternative option would be to amend Article 19 of eIDAS regulation and leave there all the aspect that will not be covered by NIS directive. Detailed analysis of both documents should be done in order to assess whether this approach is feasible.

How to deal with the issue tight relation of Article 19 and other article of eIDAS regulation*?*

The best and easiest option would be choosing the same approach as it is foreseen with financial sector and keep Article 19 within eIDAS regulation.

Not sure whether there is a simple alternative solution. To assess whether and how it would be possible to avoid such issues, detailed analysis of eIDAS regulation should be performed.

One of the issues for example would be Liability of Trust service provider (Article 13) – if Article 19 would be removed, Trust Service providers would not be liable for their services in case of issues with Network and Information systems, because Article 13 defines liability only in case of failure to comply with the obligations under the eIDAS Regulation *(if Article 19 will be removed – these requirements will not be a part of eIDAS anymore and this will dramatically lower liability of trust service providers)*.

How to deal with the issue that Network and information security requirements will not be included within conformity assessment reports?

The best option would be choosing the same approach as it is foreseen with financial sector and keep Article 19 within eIDAS regulation.

Alternative option would be defining the scope of conformity assessment reports and explicitly requiring that they would include security of Network and Information systems aspects. Of course, it would be quite difficult to do as this would require amendment of eIDAS regulation (not sure whether that could be done with directive).

How not to decrease the level of harmonisation?

All above aspects should be explicitly defined within EU documents and not left for the national legislation.

EECC and NIS 2 alignment

General observation:
We are still cautious about the removal of Articles 40 and 41 from EECC.

Specific comments:

Regarding recital 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[22] and Directive (EU) 2018/1972 of the European Parliament and of the Council[23] related to the imposition of security and notification requirement on these types of entities should ~~therefore be repealed~~ **complement 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[24].

Regarding 11.4 Article:
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 authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]**, national regulatory authorities designated in accordance with Directive (EU) 2018/1972** and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39][the DORA Regulation] within that Member State.

Accordingly, we would also suggest the deletion of **Article 40** from NIS 2 proposal, which currently aims to delete Articles 40 and 41 from EECC.

GDPR and NIS 2 alignment

General observation:
NIS 2 Proposal refers to Regulation (EU) 2016/679 but its specific timelines for notification of the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation are not transferred.

Specific comments:
For that reason, for **Article 32.1**, we would suggest:

Instead of using terminology "*within a reasonable time*", use "*without undue delay and, where feasable, not later than 72 hours after becoming aware of it*".

DORA and NIS 2 alignment

General observation:

Definitions in both these documents should be aligned. Currently there is a discrepency between the two documents, e.g. NIS 2 uses "*incident*" and, most importantly, when it comes to reporting obligations "*significant incident*" (Article 20.3); whereas DORA currently uses "*ICT related incidents*" (Articles 15 and 16) and "*major ICT-related incidents*" (Article 17).

Article 2.6 and recitals 12 and 13:

NIS 2 text clearly states the intention of financial sector to be considered as *lex specialis*, justifying that in such case, the sector-specific requirements should be "*of at least an equivalent effect to the obligations laid down in this Directive*". However, differently from NIS 2, there is currently no requirement in DORA for financial entities to report significant threats. Seeking for NIS 2 to maintain a horizontal baseline when it comes to cybersecurity requirements, regardless of a given sector, our suggestion would be to include the reporting obligation for significant cyber threats for financial entities in DORA.

CER and NIS 2 alignment:

Specific comments (Article 29.9):

Currently the cooperation between NIS 2 and CER competent authorities is not clear. Understanding that all critical and equivalent to critical entities are within the scope of NIS 2 (except for financial sector, which would have a *lex specialis status*), NIS 2 competent authorities should, in the same vein, exercise their supervisory and enforcement powers. Understandibly, in such situations NIS 2 authorities should inform CER competent authorities but the supervisory and enforcement powers of NIS 2 competent authorities should not be conditional upon request from CER competent authorities (as currently Article 29.9 suggests). Therefore, the following sentence should be deleted: "*Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent*." Instead, the following sentence could be added: "*Competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] may also request the competent authorities under this Directive to exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent*."

NETHERLANDS

Drafting proposals by the Netherlands regarding the interplay between NIS and sectoral legislation

Art.	Commission proposal	Drafting proposal	Motivation
Rec 13 [general]	(…)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. (..)	(…)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. **The financial entities covered by Regulation (XXXX/XXXX) can in addition still be asked to report incidents to the CSIRT as described in article 20 (3) of the Directive (XXXX/XXXX)** (…).	In order to maintain the role of the national CSIRT and keep the ability for the CSIRT to quickly respond to incidents the member states should have the possibility to ask financial entities to double report. Note: *The negotiations on DORA are still ongoing, the final adaptation of this recital should be in line with the final DORA proposal.*
2 (2) [eIDAS]	However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: (a) the services are provided by one of the following entities: (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; (ii) trust service providers referred to point 8 of Annex I; (iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;	However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: (a) the services are provided by one of the following entities: (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; ~~(ii) trust service providers referred to point 8 of Annex I;~~ (iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;	• Replacing the current security- and notification requirements for trust service providers with the requirements of the NIS could undermine the eIDAS-regulation and disrupts the current system of trust service provider monitoring, notification and supervision. • Therefore the eIDAS regulation should be fully maintained as a lex specialis regarding trust services. • Moreover, any issues with the current regime of trust service providers are already dealt with in the upcoming revision of the eIDAS regulation.

			• Putting parts of the eIDAS-regulation in a directive will result in de-harmonisation and will in effect create barriers for the single market of trust services.
Art. 2 (2) [EECC]	However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: (a) the services are provided by one of the following entities: (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; (ii) trust service providers referred to point 8 of Annex I; (iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;	However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: (a) the services are provided by one of the following entities: ~~(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;~~ (ii) trust service providers referred to point 8 of Annex I; (iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;	• If public electronic communications networks or publicly available electronic communications services would be subjected to the security and notification requirements of the NIS, this will lead to a change of scope of the security obligations as currently laid down in the EECC. • Besides, telecom security (availability) would also still covered by EECC (see article 108). • As long as these issues are not solved the NIS would actually not be an improvement for safeguarding telecom security and therefore the telecom regulation should be fully maintained as a lex specialis regarding ECS & ECN.
11 (4) [CER]	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 authorities ~~**responsible for critical infrastructure**~~ pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities	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** 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 Council39 [the DORA Regulation] within that Member State.	Since the CER-Directive does not use the term 'critical infrastructure', and in line with other articles in the NIS regarding the relation with CER, it is most appropriate to remove the wording critical infrastructures. Furthermore the CER-Directive only talks about competent authorities.

	Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council39 [the DORA Regulation] within that Member State.		
39 [eIDAS]	Amendment of Regulation (EU) No 910/2014 Article 19 of Regulation (EU) No 910/2014 is deleted.	~~Amendment of Regulation (EU) No 910/2014 Article 19 of Regulation (EU) No 910/2014 is deleted.~~	• Replacing the notification regime of the eIDAS regulation with the NIS regulation's regime would reduce the quality of notifications because in the eIDAS regulation the notification also applies to the connection between the offline and online part of the trust chain whereas the NIS-directive does not. • Moreover art. 19 interacts with other articles in the eIDAS regulation, such as art. 14 (liability) and art. 17 and 19 which will cease to function properly if art. 19 is removed. This will reduce the effectiveness of the eIDAS regulation without clearly identifiable benefits.
Art. 40 [EECC]	Articles 40 and 41 of Directive (EU) 2018/1972 are deleted	This article should be deleted	See above.

POLAND

I. Legal basis from the GDPR

Art. 6.1. GDPR states that:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) **processing is necessary for compliance with a legal obligation to which the controller is subject;**
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

1. **Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.**

Sensitive data

Art. 9.1 GDPR foresees that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be prohibited**.

Exemptions from this prohibition are in art. 9.2 GDPR, where among other criteria, letter **g) states that processing of sensitive data is posssible when 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**.

II. The NIS2 draft

The recital 69 states that:

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

III. Analyses

The legitimate interest is not a proper legal basis under the GDPR for processing the personal data neceesary to fulfill the tasks and obligations laid down in the NIS2, when in comes to public authorities. The competent authorities, SPOCs and CSIRTs are in most cases the public authorities. Also CyCLONe, NIS CG and CSIRT Network should be seen as a public authority.

The legal basis for data processing by the public authorities for the purposes of the NIS2 should be rather seen in art. 6.1.c GDPR (legal obligation) or art. 6.1.e GDPR **(**the public interest or the exercise of official authority)

It seems that the NIS2 foresees a legal obligations for CAs, CSIRTs, SPoCs, CyCLONe, NIS CG, CSIRT Network to perform specific task described in the NIS2. For some of these tasks it would be necessary and essential to process personal data. Therefore the legal basis from art. 6.1.c GDPR would apply.

The tasks of public authorities under the NIS are exercised for the public interest, therefore the legal basis from art. 6.1.e GDPR could also apply.

When fulfilling the obligations or exercising powers by the competent authorities or CSIRTs it might also be necessary to process the sensitive data as defined in art. 9 GDPR. As processing of such data is in principle forbidden, the competent authorities or CSIRTs to be able to process the data, should have a legal basis in the Union or Members States law only on the grounds that processing of sensitive data would be necessary for reasons of substantial public interest. It seems that there is a substantial public interest to allow processing of sensitive data when it would be essential for the incident management.

IV. The information processed while fulfilling tasks defined in the NIS2 might be also confidential pursuant to the Union and national rules (like business, telecommunication, banking confidentiality). Therefore provisions to allow processing of such data by the competent authorities, CSIRTs, SPOCs, Cooperation Group, CSIRT Network and CyCLONe for the purposes and to the extent strictly necessary to fulfil their tasks as defined in the NIS2, would support better incident handling and coordination.

V. Drafting proposal

Recital 69

(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, by entities, ~~public authorities~~, CERTs, ~~CSIRTs,~~ ~~and providers of security technologies and services~~ should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679 **and by public authorities, namely competent authorities, SPOCs, CSIRTs, NIS CG, CSIRT Network, CERTs and CYCLONe should constitute a legal obligation or the public interest or the exercise of official authority of the data controller concerned, as referred to in Regulation (EU) 2016/679.** That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, **telephone numbers, bank account numbers, geolocation data, payment data**, uniform resources locators (URLs), domain names, and email addresses.

Proposal of addition to art. 2:

Art. 2.5 a-c:

5a. To fulfil the tasks set out in this Directive, competent authorities and CSIRTs shall process personal data, including the data referred to in art. 9 of the Regulation (EU) 2016/679, and shall process information that is confidential pursuant to Union and national rules, for the purposes and to the extent strictly necessary to fulfil these tasks.

5b. To fulfil the tasks set out in this Directive, SPOCs, Cooperation Group, CSIRT Network and CyCLONe shall process personal data and information that is confidential pursuant to Union and national rules, for the purposes and to the extent strictly necessary to fulfil these tasks.

5c. When processing the personal data referred to in art. 9 of the Regulation (EU) 2016/679, competent authorities and CSIRTs shall conduct the risk analyses, introduce proper safeguards and procedures to exchange information.

SPAIN

AMENDMENT 1

Article 2 – paragraph 2 – point (a)

Text proposed by the Commission

2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:
(a) the services are provided by one of the following entities:
(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;
(ii) trust service providers referred to point 8 of Annex I;
(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;

Amendment

2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:
(a) the services are provided by one of the following entities:
(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I ***and point 6a of Annex II***;
(ii) trust service providers referred to point 8 of Annex I;
(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;

AMENDMENT 2

Annex I – table – row 8 – electronic communications

Text proposed by the Commission

— 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

Amendment

— 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.***

AMENDMENT 3

Annex II – table – row 6a (new) – Digital Infrastructure

Amendment

Sector	Subsector	Type of entity
6a 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.***

JUSTIFICATION

Micro and small enterprises of telecommunications sector must be categorized as "important entities" instead of "essential entities"

Art. 2.2.a establishes that the Directive applies to **all** public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I, **regardless of their size**. Therefore, all the operators are considered essential entities and shall be subject to ex-ante supervision.

This proposal would represent **a disproportionate increase in burden in the case of Spain, where more than 400 small local telecommunications operators are registered**. These companies lack of the necessary economic and human resources to comply with the highly demanding **ex-ante** requirements of article 29.

The general principle of exclusion of art. 2.1 leaves micro and small businesses (less than 50 employees or 10M€ turnover) out of the scope of the Directive with the aim of reducing compliance costs and administrative burden, as stated in the impact assessment. On the other hand, art. 30 establishes a reactive, ex-post supervision regime for important entities, light-touch and more proportional, "*with a view to ensuring a fair balance of obligations for both entities and competent authorities",* as elaborated in recital (70).

A more balanced solution would be **to keep micro and small enterprises providers of electronic communications services and infrastructures in the scope of the Directive, but with the categorisation of important entities**. This approach would recognize their importance as a key element in the digital infrastructures' ecosystem, ensuring their general compliance with the Directive, and at the same time minimizing administrative burden with the application of the ex-post supervision regime instead of ex-ante.

AMENDMENT 4

On Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), include the following reference in NISD2 proposal:

Add an article with this provision: **"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; will communicate to competent authority with the least possible delay the possible breaches of personal data and will cooperate to face them from their respective competences."**

AMENDMENT 5

On REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

The new proposal of a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (henceforth referred to as NIS2) is, according to the text of the proposal, fully consistent with the Regulation (EU) No 910/2014 on trust services (eIDAS Regulation). We highlight that we do not agree with this assertion, and do think the text of the proposal is not fully consistent with the Regulation.

However, the NIS2 proposal envisions the repeal of the provisions laid down in the eIDAS Regulation related to the imposition of security and notification requirements on trust service providers. Article 39 of the NIS2 proposal deletes Article 19 of Regulation (EU) No 910/2014, and its provisions are superseded by those of the proposal for all trust service providers referred to point 8 of Annex I of the NIS2 proposal, including micro and small entities within the meaning of Commission Recommendation 2003/361/EC of 6 May 2003. The NIS2 proposal seeks to repeal the entire supervisory mechanism instituted by Regulation (EU) No 910/2014 on trust services (eIDAS Regulation), including these as a subsector of "important entities".

We most strongly oppose the provisions laid down in NIS2 proposal concerning trust services. **We strongly request that trust services be eliminated as a subsector of essential entities in application of the principle of lex specialis**, as in the current Directive.

The following paragraphs detail the three most problematic aspects of the provisions laid down in NIS2 proposal concerning trust services.

- First, the scope of assets to be supervised in the eIDAS Regulation is broader than that of the proposed Directive NIS2. The proposal is limited to the security of the information systems and networks that the entities use in the provision of services. The eIDAS Regulation supervises all dangers with an impact on the security of the trust service, from the Registration Authority (normally its network infrastructure will be from another company) to the procedures executed in the user environment and the user environment and its communications. For example, it also supervises the provision of the service itself (eg issuance of the certificate), as well as the use of the products (eg that certificate) that would be within the scope of the user. This derogation implies a removal of this security supervision.

The proposal refers only to ""the security of network and information systems which those entities use in the provision of their services"". It does not cover the security of issued certificates or smart cards, which do fall within the objective of article 19 eIDAS. ""Qualified and non-qualified trust service providers shall take appropriate technical and organizational measures to manage the risks posed to the security of the trust services they provide."". The security imposed by art. 19 of the eIDAS Regulation to trust services has a greater scope than the physical and logical infrastructures of the provider, to which the NIS2 proposal is limited. Under the proposal, an incident as serious as ROCA would not be reported.

- Second, the inclusion of the sector in the proposal gives the Member States the possibility to demand different technical security measures, when the eIDAS Regulation and its implementing acts impose common ones. It is precisely this fragmentation that motivated the conversion of the Electronic Signature Directive into the current eIDAS Regulation. The NIS2 proposal, in its article 18 (Cybersecurity risk management measures) places in the hands of the MS the cybersecurity measures that essential and important entities must take to ensure a level of security of their networks and information systems. The NIS2 only imposes very vague general guidelines on EMMs in this regard (""The measures referred to in paragraph 1 shall include at least the following: ..."""). This is not the case in the eIDAS Regulation. Article 24 2 of eIDAS says, for example, in section e) that suppliers must use reliable systems and products that are protected against any alteration and that guarantee the security and technical reliability of the processes they support. And section f) says that they have to use reliable systems to store data.
- Third, the proposal applies the toughest supervisory regime to all companies in the sector, even small and micro-companies. The eIDAS Regulation has an ex ante supervision regime, similar to that of ""essential entities"", for qualified trust service providers and an ex post, similar to that of ""important entities"", for non-qualified ones. This follows the unanimous criterion of the supervisory authorities of the MS, who judge this level of supervision adequate to the relative importance of each provider. This tightening would have a pernicious effect on companies in the sector, undermining their already diminished competitiveness vis-à-vis suppliers from outside the EU."

AMENDMENT 6

On REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), include the following reference NISD2 proposal:

Add an article with this provision: **“The competent authority and the authorities responsible for data protection; referred to in on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); they will communicate with the least possible delay the possible breaches of personal data and will cooperate to address them from their respective competences.”**

AMENDMENT 7

On Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

Article 11 Cooperation at national level

Amendment: Add a new section 11.6 with the following text: "**For the purposes of simplifying the reporting of security incidents, Member States should establish a single-entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC.**"

Justification

Regarding the notification of incidents, DORA (art. 17) includes the obligation of banking entities to notify serious incidents to the competent authority of the financial sector, which in turn will notify the European Banking and Financial Authorities and the NIS Single Point of Contact, establishing an incident notification procedure that could be parallel to that established by the NIS Directive.

However, DORA proposal does not include the CSIRT network in the notification process. This network has been in place for several years, is getting a high level of maturity and a lot of resources has been invested by the EU and Member States.

Recital 56, for the purposes of simplifying the reporting of security incidents, includes that: "*for the purposes of simplifying the reporting of security incidents, Member States should establish a single-entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC*."

This idea must be included in the articles. Article 11.1 only requires the coordination of authorities at a national level, but it does not impose this single entry point. It is very important to keep this point, and it represents a solution for other legislations and authorities, such as DORA. This national single point would distribute the information among the involved authorities and CSIRTs.

SWEDEN

As the proposal is still being analyzed, these positions are not exhaustive.

Sector-specific acts

SE supports that NIS2 should constitute a horizontal directive containing minimum security requirements across all sectors and recognises the need for sector specific rules for certain sectors. In order to achieve an effective NIS "eco system", it is vital that NIS is clear on how necessary interaction between NIS and sector regulations is safeguarded and also, how the various sectorial legislation will relate to each other. Otherwise, as further sectorial legislative frameworks are developed, there is a risk that the horizontal overview is lost. Since different sectors often are interconnected in various ways, a fragmentation of the eco system would jeopardize the very essence of NIS, i.e. to ensure a high common level of cybersecurity across the Union.

How to achieve this goal needs careful consideration. For example:

Incident reporting: How to achieve cost efficient reporting, avoiding double reporting while ensuring the horizontal oversight at NIS-level, having in mind that incident reporting could be spread between different national authorities, competent under different sectorial regulations.
How to handle situations when entities might fall both under the scope of sectorial legislation and NIS (for example critical third-party providers in DORA and digital service providers in NIS).
Need for secure information sharing on national and EU-level.
Need for coordination between sector specific authorities and NIS-authorities (and where relevant EU-authorities).

There might be different ways to take on board these issues. Either by introducing general principles in NIS to steer the way forward or to include detailed references. At the same time, overly complex and costly systems should be avoided, and flexibility must be remained. SE welcomes further discussions on this issue.

Regulation of digital operational resilience for the financial sector (DORA)

It is important to ensure coordination between DORA and NIS2 and the relevant authorities regarding digital infrastructure (Annex 1, sector 8). Entities defined as essential entities under the sector Digital infrastructure may also be defined as a critical third-party service provider under DORA. DORA is lex specialis in relation to NIS2 only for financial units and not third-party service provider – which means that entities under sector Digital infrastructure will be covered by supervision according to NIS2 but can also be subject of overview according to DORA. Steps have been taken in the DORA-negotiation to ensure necessary coordination between relevant NIS- and DORA-authorities; it is necessary to investigate the need for clarifications also in NIS in this regard.

General Data Protection Regulation (GDPR)

A comprehensive article regarding Data Protection Regulation should be added to the NIS2 Directive stating that the personal data must comply with the Unions data protection legislation.

Directive of the European Parliament and of the Council on resilience in critical entities (CER)

Recital 14:

Since there may be more competent authorities than two under both directives that should cooperate, and exchange information SE suggest amending the last sentence in recital 14 to: "~~**Both**~~ The authorities should cooperate and exchange information for this purpose."

In terms of clarity SE considers it valuable if NIS2 included the definitions for "critical entity" as well as "entity equivalent to a critical entity" in Article 4 in NIS2, by cross-referencing to definitions in the CER directive. We propose to add 4.27 and 4.28 for these purposes.

In order for the wording in art. 11.5 to more fully correspond with recital 14, as well as with the corresponding article to 11.5 in CER (art. 8.6), SE suggests the following drafting proposal:

Member States shall ensure that their competent authorities regularly **cooperate and exchange** ~~provide~~ information ~~to~~ with 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.

European Electronic Communications Code (EECC) and the regulation on electronic identification and trust services (eIDAS)

1. Sweden's position is that neither electronic communications services and networks (telecom services) nor trust services should be included as new sectors in the proposed NIS2 at this point.

<u>EECC, eIDAS and NIS 2 – different scopes and national differences</u>

The inclusion of new sectors, previously regulated in legal frameworks with a different focus than NIS2, raises questions concerning where to draw the line on what is and is not regulated. This is most notably relevant when it comes to telecom services as well as trust services.

In general, to streamline the different frameworks, it is not sufficient to simply move articles from one legal text to another; further harmonisation and elaboration is needed to make sure that the scopes are merged or that new scopes that are moved in to the NIS2 are preserved.

The current scope of the EECC is not limited to a telecom provider's network and information systems. Rather, it is meant to encompass the electronic communication service (or network) as a whole. There could be a gap between the *telecom services* currently regulated in the EECC, and the *network and information systems* regulated in the NIS framework**.** Moving the security provisions of the EECC to NIS2 could therefore have a negative effect on the security of networks and services due to differences between NIS 2 and EECC. Including telecom as a sector in NIS2 could create uncertainties.

<u>Moving the security provisions of EECC to NIS 2</u>

It is important to maintain regulations that safeguard telecom security in areas outside the NIS Directive's scope of network and information systems. The current scope of the EECC is not limited to a telecom provider's network and information systems. Would, for example, a telecom

provider's customer service (responsible for proper authentication etc.) be regarded as a part of the network and information systems used to provide the essential service telecom? A SIM swap attack, targeting a telecom provider's customer service, would most likely not give an attacker access to more than a single subscriber's subscription information – in other words: only the essential service itself (telecom), and not the network and information systems used in the operations. There are other examples of telecom services regulated in the EECC that probably would not fall within the scope of NIS2: enterprise switchboard services, different IoT solutions such as connected home appliances, etc.

Simply put, there seems to be a gap between the electronic communications networks and services currently regulated in the EECC, and the network and information systems regulated in NIS2.

Moving the security provisions of eIDAS to NIS 2

NIS2 suggests, *inter alia*, that trust service providers (TSP's) referred to in Art 3(19) of the eIDAS Regulation be included in the scope of the NIS2 and that Art 19 of the eIDAS Regulation be removed and replaced with the security requirements of NIS2. SE position is that trust services should not be included as new sectors in the NIS Directive at this point.

The conversion of a regulation to a directive

Trust services and TSP's are currently regulated in an EU Regulation, and subsequently the provisions are directly applicable without the need for national implementation., harmonisation will hardly increase when replacing a Regulation provision with a Directive provision. By deleting Art 19 of the eIDAS Regulation it is possible that harmonisation could instead decrease, with some national laws resulting in stricter security provisions than others.

The inclusion of eIDAS in NIS2 would divide an existing trust and security framework

The eIDAS Regulation constitutes a framework that regulates different aspects of security for TSP's. While Art 19 is the provision that establishes security requirements for TSP's, it is not isolated from other provisions in the eIDAS Regulation in terms of interpretation and application.

To give some examples, Art 24 contains requirements for qualified TSP's (QTSP's), and the assessment of measures taken under this article is in no small part related to the application of Art 19. Moreover, Art 13 sets up rules for liability for TSP's, stating that they are liable for damages caused due to a failure to comply with the obligations of the eIDAS Regulation. Art 19 is, once again, relevant for the application of Art 13. Interpreting and applying the provisions of the eIDAS Regulation means looking at the framework as a whole; removing Art 19 might result in the framework becoming less than the sum of its parts.

Further, the focuses of the eIDAS Regulation and the NIS framework are different, the latter with a specific emphasis on security of network and information systems. Art 19 of the eIDAS Regulation states that the security measures are meant to manage the risks posed to the *security of the trust services provided*. In contrast, Art 18 of NIS2 asserts that the security measures should manage the risks posed to the *security of network and information systems which those entities use in the provision* of their services. Trust services do not only exist and function in a digital context; the identification of a natural or legal person may, for example, include physical verification. NIS2 has a clear focus on cybersecurity while the eIDAS Regulation arguably encompasses other aspects of security and trust. Removing Art 19 from the eIDAS Regulation would be dividing up an existing trust and security framework, with its own focus and context. This split could cause difficulties in the interpretation and application of the rest of the eIDAS Regulation, as well as confuse the scope of the security requirements for TSP's.

Different supervision frameworks in the eIDAS Regulation and NIS2

According to the eIDAS Regulation, the supervisory body may exercise supervision of QTSP's through *ex ante* and *ex post* supervisory activities.[6] Supervision of non-qualified TSP's may, on the other hand, only be subject to *ex post* supervision.[7] Under NIS2, all TSP's will be considered essential entities in accordance with point 8 of Annex I. Supervision for essential entities under NIS2 can be exercised through both *ex ante* and *ex post* supervision.

While it is possible that there might be benefits to allowing *ex ante* supervision for nonqualified TSP's, it can be cost driving and inhibit innovations if nonqualified TSP's also are to be covered by ex ante supervision. The fact that there could be two different supervision provisions for the same entities might cause confusion and an administrative burden for the TSP's. Additionally, NIS2 may lead to TSP's being under the supervision of two different supervisory bodies. This could result in fragmentation rather than harmonisation, as Member States could organise their supervision differently from each other.

---

6 Art 17.3 (a), the eIDAS Regulation.

7 Art 17.3 (b) the eIDAS Regulation.

Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 17 May 2021

WK 6380/2021 INIT

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI
PROCIV

WORKING PAPER

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
N° Cion doc.:	14150/20 [COM (2020) 823 final]
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148: interaction with sectoral legislation - Comments by AT, BG, CZ, DK, EE, FI, FR, DE, IE, IT, LT, NL, PL, ES and SE delegations

Delegations will find in Annex comments by AT, BG, CZ, DK, EE, FI, FR, DE, IE, IT, LT, NL, PL, ES and SE delegations on the above-mentioned subject.