Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 22 March 2021

WK 3965/2021 INIT

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI

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
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 - Comments by BE, CZ, DK, EE, FI, FR, DE, EL, IE, IT, LV, LT, LU, NL, ES and SE delegations on Articles 20, 22 and 23

Delegations will find in Annex comments by BE, CZ, DK, EE, FI, FR, DE, EL, IE, IT, LV, LT, LU, NL, ES and SE delegations on Articles 20, 22 and 23.

TABLE OF CONTENT

BELGIUM

Disclaimer:
The list of questions below is non-exhaustive and might be further expanded.

Art. 20 – Reporting obligations

20 (1): *…notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of **any incident having a significant impact** on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the…*

- In order to be compliant with the Belgian situation, anytime a reference is made to "notify the competent authorities or the CSIRT", the text should be changed into "notify the competent authorities and/or the CSIRT".

(Art. 20 (2)) – Significant cyber threats

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

- Paragraph 3 of Article 20 only explains when an incident can be considered to be significant, but a "significant cyber threat" is not defined?
- Wouldn't it be useful to add a non-exhaustive list of examples of such significant threats?

(Art. 20 (3)) – Significant incident

20 (3): *An incident shall be considered significant if:*
*(a) the incident has caused or has the **potential** to cause **substantial** operational disruption or financial losses for the entity concerned;*
*(b) the incident has affected or has the potential to affect other natural or legal persons by causing **considerable** material or non-material losses.*

- Can the terms *significant, potential, substantial and considerable* be clarified, or could it be specified that these are up to the member states to decide? These terms now seem to obfuscate the threshold of when an incident needs to be notified.
- If these thresholds are up to member states to decide, does this not risk to potentially expose entities that are active in more than one member state to different reporting obligations in different Member States (which does not only go against the intent of the Directive to harmonize such obligations, but also clouds the exact relation with equivalent requirements in sectorial legislation)?

(Art. 20 (4) a & c) – Reporting to competent authorities or CSIRT

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

- Could it be clarified why within 24h? Does the experience not learn that 24h is often too early to know what exactly is going on, and therefore whether there might be malicious action?
- How does the Commission match the flexibility provided by the description in Recital 55 with the strict formulation ("in any event within")?
- It would be important for the entities to limit strictly the number of incident notification templates, notification ways, and recipients in order to keep the process manageable. We should take into account the fact that reporting is an additional task during a crisis/incident management process and so that multiple incident notifications would be difficult to manage in a short period of time. For example NIS2 and DORA should organize their incident notification process as integrated as possible for the entities, avoiding unnecessary double tasks.
- Is there a reason for the delay to be different from delays for incident notifications applicable within the framework of other European directives (e.g. 72 hours after having become aware of the data breach to notify the competent authorities for GDPR-incidents), while the directive proposal stresses the importance of alignment & coordination with other EU law?
- Given the fact that it's sometimes hard to evaluate the exact beginning of an incident, especially in the case of a cyber fraud or malware, wouldn't "without undue delay ~~and in any event within 24 hours after having become aware of the incident~~" be a more appropriate formulation?
  A short delay could be very difficult to respect when all the resources of an entity are focused on the resolution of a crisis.
- Also: does this provision apply to the entire art. 20(1), so including the possible cross-border impact?
- It would be useful to indicate the objective or purpose of each of the measures under 20(4). What will each of the reports trigger or contribute to?

a final report not later than one month after the submission of the report under point (a)

- Could it be clarified why within one month? Would it not be better for the final report to be sent only when the full extent of the incident is known, which sometimes cannot happen within one month?

(Art. 20) in relation with Recital (56)– Single entry point for notifications

Whereas recital (56) mentions
Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, 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. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.*

- Has any initiative already been initiated to shape, define or develop such *single entry point?*
- Does the Commission consider an option where such national single entry point is part of an integrated or at least interconnected Union system, so that the single entry of a cross-border incident in one Member State results in the notification of all concerned Member States f.e.?
- Does the Commission consider the development and implementation of a reporting tool (based on the database of such *single entry point(s))* for the generation of (automatic and uniform) reports as those required by 20 (9)?
- It would be important for the entities to limit strictly not only the number of incident entries, but also the number of incident notification templates, notification ways, and recipients in order to keep the process manageable. We should take into account the fact that reporting is an additional task during a crisis/incident management process and so that multiple incident notifications would be difficult to manage in a short period of time. For example NIS2 and DORA should organize their incident notification process as integrated as possible for the entities, avoiding unnecessary double tasks

(Art. 20 (5)) – CSIRT response

The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity

- Given the potential large increase in the number of entities that should report significant incidents, could this specific obligation not place a significant extra burden on CSIRTs to reply, even to notifications that do not request further assistance or are clearly not malicious?
- Can the response also consist of (only) a receipt confirmation in such case?

(Art. 20 (9)) –Summary Report for ENISA

The single point of contact shall submit to ENISA on a monthly basis a summary report

- Could it be clarified why every month? Would a quarterly reporting not suffice, and allow the staff of CSIRTs and competent authorities to focus on mitigating the incidents?
- Might one month not be relatively short to a) know the full extent of an incident; b) give competent authorities and CSIRTs enough time to process the data?
- Does this imply all initial notifications or only the full reports?
- How much time would SPOC's have to send in the report? The final report on an incident that was initially notified at the end of month X might under art. 20(2)c only be available at the end of month X+1

(Art. 20 (11)) – Implementing acts

Commission, may adopt implementing acts

- Might the extra specifications in such implementing acts not jeopardize established equivalencies in obligations between NIS.2 and sectoral legislation?

Art. 21 – Use of European cybersecurity certification schemes

The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate

- As the entities depend on suppliers, can suppliers also be required to obtain a certificate?
- What is the COM opinion on suppliers from non-EU countries that provide critical IT services/products to essential entities in relation with obligations of certification? What provisions concerning jurisdiction/ territoriality apply for the suppliers?

Art. 22 - Standardisation

In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

- Does the Commission have in mind to ever converge towards one single preferred or towards one specifically-developed EU standard, or is co-existence of several standards a base assumption?

Art. 23 – Databases of domain names and registration data

- Could the Commission clarify to what extent these obligations are novel, compared to existing obligations for TLD registries and domain registration services.
- This article proposes measures that can clearly mean an extra protective factor for the overall cybersecurity, especially focusing on the repressive/reactive side of the spectrum. Is it not the case, however, that many (if not most) threats come from non-European TLDs, which are not in scope?

(Art. 23 (1)) – Domain Name registration data- data protection

Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data

- Only (and all) of the TLD registries in the scope of the directive (art.2-2-a-iii)?

(Art. 23 (2)) – Domain Name registration data – contact info

Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information ***to identify*** *and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.*

- How should TO IDENTIFY be interpreted?
  If this is transposed into an identification obligation, then registry operators and registrars must have access to the legal tooling to allow them to identify people, organization, companies, etc... taking into account the international nature of the DNS ecosystem, the technologies available and the economic impact.

(Art. 23 (4)) – Domain Name registration data *-publication*

Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data

- Does publish mean: available to the entire public?
- Relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs is not PUBLISHED but can be CONSULTED ON DEMAND through different interfaces with different security controls. We assume that Art 23 (4) refers to what today is understood under the label of "WHOIS data".
  Is this assumption correct?

(Art. 23 (5)) – Domain Name registration data -access

Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provides access to specific domain name registration data upon ***lawful and duly justified*** *requests of* ***legitimate access seekers****, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available*

- The term "legitimate access seekers" must be defined precisely.
- Further clarification as to what constitutes a "lawful and duly justified" request based on which access shall be granted, and under which conditions. Ideally, Member States foresee a framework to vet requests and identify "legitimate access seekers" effectively levelling the playing field for all involved parties by establishing the rules of engagement.

CZECH REPUBLIC

ART. 20

Regarding the Art. 20 we would like to ask why in para 1 is used term incidents having a significant impact, but in para 2 is the definition of incident, which shall be considered significant. We propose to unify those terms. We welcome the level of specificity of the definition of significant incident, and we would like to know more about plans and content of the implementing acts referred in para 11. Regarding para 6, we would like to know why the competent authority or CSIRT in case of incident, which concerns two or more MS, inform just the affected MS and ENISA, why not the CSIRT´s network?

DENMARK

Pertaining to the next meeting on the revised NIS Directive on March 24th concerning **articles 20, 22 and 23,** please find the Danish questions and comments listed hereinunder:

Art. 20 (Reporting Obligations)
Art. 20 § 3 – "considerable" - **whose definition of the term "considerable" is being used? (The competent authority? The CSIRT? The entity itself?) / i.e. who have final say in determining the threshold, and thus deciding which incidents are significant? (e.g. by whose definition is a material loss "considerable")?**
Art. 20 § 3 – "material and non-material losses" - **by which definition? Non-material losses could mean many things: e.g. loss of security, loss of trust. Are those included?**
Art. 20 § 3 – "significant incident" – **why is this concept being defined here, and not in article 4, where all of the other concepts in the directive are being defined?**
Art. 20 § 6 – "confidentiality" – **could the Commission possibly elaborate on the thoughts behind, why confidentiality is only bein mentioned in connection with international reporting (and not also in connection with national reporting)? (I.e. which balances/conflict of interest are at play, and why did the balance ultimately come out this way?)**

Art. 23 (Databases of domain names and registration data)
We are seeking clarification on 3 subtopics:
1) the division of responsibilities between TLD registries and the entities providing domain name registration services for the TLD (registrars), including whether the provisions entail duplication of work
2) jurisdictional issues and
3) which domain name registration data must be collected and published.

Re 1 (Division of responsibilities)
The proposal requires Member States to ensure, among others, that TLD registries and registrars collect and maintain accurate domain name registration data in databases and publish the registration data in compliance with GDPR.

- **If it is already required in national law for a TLD registry to collect and publish registration data, as required by the proposal, would there still be an obligation for registrars under that TLD to ensure the accuracy of the registration data and publish the registration data?**

Re 2 (Jurisdictional issues)
- **Are TLD registries also subject to the rules of jurisdiction in Article 24 for the provisions under article 23? If so, why do the same jurisdiction rules not apply to registrars?**

- **Do the provisions of Article 23 also apply to entities outside the EU?**

- **Do the provisions of Article 23 apply to a registrar established in the EU when a registrant resident outside the EU acquires a domain name at a TLD registry established outside the EU?**

Re 3 (Registration data)

- **In view of the challenges that have arisen with WHOIS data in ICANN after the GDPR came into force, why does the proposal not specify which data elements that as a minimum must be collected, respectively published?**

ESTONIA

The following list of comments and questions is non-exhaustive and may be expanded in future discussions.

Article 20 Reporting obligations

Estonia welcomes the overall harmonised approach for incident reporting that was chosen for the proposal of the directive.

Art. 20 para 4) – do entities need to provide a final report with detailed information on near misses or threats, for which an initial notification was sent, but which later turned out to be inconsequential?

Art. 20 para 9) – we propose to set up a submission of a quarterly (instead of monthly) summary report of incidents – this would allow ENISA to draw conclusions on trends that are more substantial, while not overburdening both SPOC-s and ENISA.

FINLAND

Article 20

- In general, we want to highlight the importance to ensure coherence between these obligations and reporting obligations to data protection authorities according to GDPR. We support cooperation and information exchange between national competent authorities of NIS2, CER and DORA to enhance situational awareness.

- Art. 20 (1) It is important that essential and important entities receive targeted information on the reporting obligations and processes.

- Art. 20(4) It is important that the initial notification is issued as swiftly as possible (within 24h).

- We support simultaneous reporting to the competent authority (obligatory) and CSIRT (on voluntary basis). In Finland this has proven to work well based on good and trusted cooperation between CSIRT, competent authorities and the entities. We want to enhance this cooperation and build on existing trusted channels.

- Still, excessive administrative burden to entities in regards reporting obligations should be avoided. Duplication in terms of reporting to authorities should be avoided. National leeway for more detailed arrangements is very important.

- Art 20(4)(b): It is important that issuing an intermediate report does not burden the entities in situation of incident/crisis. This is especially important to entities with more restrictive resources.

- Art 20(8): It is important that such exchange of information follows adequate classification and trusted channels when handling sensitive information.

- Art 20(9): This reporting should be further clarified. It is important that such reporting does not burden CSIRTs and SPOCs in their operational activities (e.g. incident handling) especially in smaller MS.

FRANCE

Dans la perspective de la réunion du groupe horizontal sur les questions cyber du 24 mars 2021, les autorités françaises souhaitent partager avec la Présidence des premiers éléments d'analyse sur la proposition de directive en objet. Les autorités françaises tiennent cependant à souligner que l'analyse du document à l'échelle nationale se poursuit et que ces éléments pourraient être appelés à évoluer au cours des négociations.

Sur l'**article 20**, les autorités françaises soulignent à titre liminaire, que la proposition de directive étend considérablement les obligations de notifications, tant sur la charge incombant aux opérateurs qu'aux États membres. Elles s'interrogent donc sur le caractère réaliste de la bonne mise en œuvre des mesures prévues par cet article. À titre d'exemple, la qualification d'un incident exige du temps (en général bien plus que 24h). Par ailleurs, de telles dispositions ne pourront être mises en œuvre que si les autorités nationales disposent d'une vision claire et précise des opérateurs régulés. Ceci plaide donc une nouvelle fois en faveur de l'introduction d'un mécanisme de déclaration des opérateurs auprès de leur autorité de supervision, comme les autorités françaises ont déjà eu l'occasion de le souligner.

Plus spécifiquement, les autorités françaises :

- s'interrogent quant à savoir si les dispositions prévues par cet article s'appliquent également aux filiales des entités essentielles et importantes ;
- souhaitent obtenir des éclaircissements sur ce qui est entendu au considérant 69 et les implications éventuelles de ce considérant à l'article 20 ;
- interrogent la Commission européenne sur les raisons ayant motivé :
    - une reformulation substantielle des paramètres définissant un incident significatif : la directive sur la sécurité des réseaux et des systèmes d'information (NIS) originelle était à cet égard plus précise et ne nécessitait donc pas un travail législatif supplémentaire à travers l'adoption d'acte délégué (tel que prévus au paragraphe 11) ;
    - le recours à des actes d'exécution pour définir le format et les procédures de notification prévus aux articles 1 et 2.
- soulignent qu'avec l'abrogation de l'article 19 du règlement sur les services d'authentification et de confiance en matière d'identification électronique (eIDAS (UE) n° 910/2014), prévue par l'article 39 de la directive NIS, la remontée d'incidents des PSCO[1]/PSCQ[2] vers l'autorité nationale est supprimée. Les autorités françaises souhaitent interroger la Commission sur les raisons ayant motivé cette décision et la bonne articulation avec le règlement eIDAS, dont la proposition de révision est attendue dans les prochainement ;

1 Prestataires de services de confiance.
2 Prestataires de services de confiance qualifiés.

- indiquent que la notification d'un incident impactant un ou plusieurs États membres de l'UE prévue au paragraphe 6, constitue par nature un échange d'informations sensibles. Ainsi, fournir automatiquement le même niveau de détails à l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pose question, particulièrement en l'absence de réseaux de communication sécurisés.

Concernant les **articles 22 et 23**, les autorités françaises n'ont pas de commentaires à formuler.
Les autorités françaises se tiennent à la disposition de la Présidence portugaise pour toute précision utile.

GERMANY

Please note: The following list of comments and questions regarding Art. 20, 22 and 23 NIS2 is non-exhaustive and may be expanded in future discussions. Comments and questions are sorted by order of the Articles.

1. Question regarding Art. 20 (in general – cost) – Could the Commission kindly provide some background on the expected administrative burden on essential and important entities with regard to the reporting obligation?

2. Question regarding Art. 20 (in general – delegated acts) – Could the Commission kindly elaborate on the need for implementing acts specifying the type of information, the format and the procedure of incident notifications? In light of the expected increase in incident notifications, it seems necessary to optimize / streamline the existing national incident notification procedures during NIS2 transposition. Introducing implementing acts further specifying or altering these provisions at a later stage during NIS2 transposition could lead to additional expenditures and duplicate work. The same would apply to specifying the term "significance" in the post-implementation period. Could the Commission kindly explain why it has chosen not to specify "significance" pre-implementation if it already expects post-implementation regulation?

3. Comment regarding Art. 20 (in general – notifications) – As already mentioned in the context of Art. 2, the interplay with NIS2 and possible *lex specialis* cybersecurity incident notification mechanisms (e.g. DORA) requires clarification. In Germany's view, *lex specialis* notifications need to always also include immediate access to incident notifications for national competent authorities under the NIS2 directive. This can be achieved by, for example, automatic and direct access to the incident notifications through a common reporting mechanism, automatic and direct forwarding of the notifications to the NIS2 national competent authority by the sector specific competent authority. However, double reporting duties for the industry should be avoided.

4. Question regarding Art. 20 (in general – notifications) Germany welcomes the general notion of making notification procedures for security incidents as efficient as possible. However, the relationship of Art. 20 NIS2 to the notification obligation under Art. 33 GDPR is unclear in those cases, in which an incident under Art. 20 NIS2 encompasses a personal data breach. In the event of a personal data breach, the data protection supervisory authority must be informed within 72 hours (*cf.* Art. 33 para. 1 sentence 1 GDPR). According to Recital 56 NIS2, member states should even create a "*single entry point for all notifications*" of "*security incidents*". We kindly ask the Commission to clarify, if in its opinion a notification via such "*single entry point*" is compatible with the wording of Art. 33 para. 1 sentence 1 GDPR (notification to the "*supervisory authority competent in accordance with Article 55*"). Because in such cases, notification would not made directly to the data protection supervisory authority. Furthermore, cases of a breach of personal data may not concurrently constitute a security incident? Should in the Commission's view a notification in such cases also be made via the "*single entry point*"? If not, what is in the Commission's view the added value of such "*single entry point*" for the entities concerned?

5. Question regarding Art. 20 (in general – notifications) – In light of the considerable increase of the number of entities within the scope of NIS2, the notification obligation appears ambitious. From a procedural point of view, it appears doubtful to be able to maintain the current reporting system (from the NIS1 Directive) while at the same time greatly expanding the group of persons affected. Could the Commission kindly elaborate if in drafting Art. 20, the possibility to rely on a more automated notification process was assessed? The contents of notifications required by Art. 20 appear not to be suitable to be processed by an automated system.

6. Question regarding Art. 20 para. 1 – No member state should be obligated to share information, the disclosure of which would be in conflict with its essential security interests. Does the Commission agree that a respective clarification should be added?

7. Question regarding Art. 20 para. 3 – Could the Commission kindly give some examples of incidents that are not significant? It is very difficult to imagine an incident occurring in an important or essential entity that would have not the potential to affect other natural or legal persons by causing considerable material or non-material losses.

8. Question regarding Art. 20 para. 1 sentence 2 – Could the Commission kindly clarify the legal nature of the provision with regard to notification of recipients of services. Form the wording ("where appropriate") it is not clear if this is (i) to constitute a legally binding obligation for entities under certain circumstances (if so, which?) or (ii) a non-binding guidance. Furthermore, how does the Commission envision the respective process in practice and which benefit is to be achieved by it?

9. Question regarding Art. 20 para. 4 lit. c – Could the Commission please elaborate on the obligation to provide a final report within one month? In practice, incident handling in general and identification of the root cause oftentimes require periods longer than one month. Kindly also elaborate on how the Commission weighed the respective cost increases for entities against potential benefits.

10. Question regarding Art. 20 para. 5 – Could the Commission please give some details on the scope of technical support to be provided upon request? In light of the significant increase of entities in scope of the directive, this may require significantly more resources.

11. Question regarding Art. 20 para. 6 – We kindly ask the Commission to provide an overview of the changes imposed by NIS2 on notifications between member states and elaborate on the motivation that lead to these changes.

12. Question regarding Art. 20 para. 9 – The provision provides for a monthly reporting obligation for NCAs *vis-à-vis* ENISA. Could the Commission kindly provide details on the intended use case for the data and benefit of this exercise? Could the Commission please clarify the scope of the "guidance on the parameters" to be issued by ENISA? Would such guidance possibly mandate including information in reports that may lead to the identification of an individual case or the notifying entity?

13. Comment and question regarding Art. 23 (in general) – The provision is very vague concerning the completeness of the personal data (see para. 1), categories of personal data involved (see para. 2) and the conditions for access to the data (see para 5). Could the Commission kindly elaborate why it has refrained from drafting a more detailed provision, in order to establish a minimum standard across the Union in this regard? In particular, could the Commission please clarify what is to be understood by "legitimate access seekers" and "duly justified requests" (para. 5)? In general, it should be ensured that claimants are not burdened with disproportionate costs when they are lawfully asserting their claims. An addition to Art. 23 or in the recital seems appropriate (para. 6).

14. Question regarding Art. 23 para. 1 – Why has the Commission chosen the wording "with due diligence subject to Union data protection law" instead of "in accordance with (…)"?

15. Question regarding Art. 23 para. 3 – With regard to proportionality, will there be a distinction between assuring the accuracy of new registration data and the high amount of already existing registration data? With regard to mentioned policies and procedures for registration processes, does the provision effectively mandate horizontal identity checks on every registrant or does it allow a risk-based approach, e.g. relying on smart solutions and a case-by-case basis?

GREECE

Art. 20

20 (3). "*An incident shall be considered significant if:*
(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned; (b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses"

- Is our understanding correct that the aforementioned criteria may be further specified according to national legislation, incl. specific conditions or potential thresholds for the significance of the incident?
- Is our understanding correct that the criteria of significance referred to in this paragraph constitute *minima,* which shall allow the Member States to broaden the obligation of notification of incidents to the competent authorities by national legislation?

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

- Could you provide examples of such "duly justified" cases?

20 (5): "*Where the CSIRT did not receive the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in collaboration with the CSIRT."*

- We consider that such circumstances and obligations of collaboration between national competent authorities, incl. CSIRTs, is an issue to be addressed more appropriately by national legislation and not the EU law.

The CSIRT shall provide additional technical support if the concerned entity so requests."

- Instead of "shall provide" we propose the wording "may provide". In addition, the conditions and modalities of such a technical support should be specified by national legislation

20 (7): Regarding the publicization of incidents we consider the wording of NIS 1.0 as more appropriate:

"the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident."

20 (11): *"The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of the notification submitted pursuant to paragraphs 1 and 2."*

- We consider that the issuing of such acts requires the consent of the Member States

Art. 23

23 (2): "*Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs"*

- "*contain relevant information":* This wording should be more specific. What information should be contained?

23 (5): "*Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law"*

- With respect to the Union data protection law, we consider that the access to such data should be granted by nationally designated competent authorities that shall examine the legitimacy of the request, following a procedure defined by national legislation.

IRELAND

Article 20

What linkages if any are there with Article 7? Is a large scale incident an incident having a significant impact requiring notification under Article 20?

20.1

How wide is the scope with "any incident having a significant impact on the provision of their services"? While 'incident' is defined and reference is made to para3, 'services' is not clear. Does it mean the entirety of the organisation's business or function or limited to that set out in Annex 1 and 2?

What is meant by "recipients of their services"? What precisely should be notified? An obligation on essential and important entities to share incomplete information about an event or disruption needs to be carefully worded. Furthermore the blanket application of this requirement may work in favour of large global players who already have public domain dashboards. Is this proportionate and scalable for medium, small and micro sized businesses?

What is meant by "without undue delay" here when 24 hours is referenced in para4?

How can Member States ensure that entities report information enabling the determination of cross border impacts of an incident?

20.2

What precisely is a "significant cyber threat"? Can the Commission provide examples? Is it public domain information, based on open sources, such as around various campaigns? Is for example 'Solar Winds' a significant threat or a significant incident? It may be an actual event for some but a potential circumstance, event or action for others.

How is reporting threats legally enforceable since they are not event related? Organisations can have different risk appetites and therefore differing approaches as to what constitutes a 'significant threat'. Could a threat constitute known unpatched vulnerabilities in an organisation's network and information system?

What is meant by "recipients of their services"? What precisely should be notified? An obligation on essential and important entities to share incomplete information about a threat needs to be carefully worded. Can the Commission give an example where feedback on a significant cyber threat should be given to recipients of services? How would this be appropriate in the absence of measures been taken by essential and important entities to reduce the threat and which result in scheduled disruption/maintenance to services for others? Is this proportionate and scalable for medium, small and micro sized businesses?

What is meant by "without undue delay" here when 24 hours is referenced in para4?

20.3

What is meant by "substantial operational disruption"? Is this about disruption directly impacting users of essential and important entities? What is meant by 'financial losses'? Any interruption in services incurs financial costs. What precisely is meant by 'substantial'? A loss of service providing account based email for a few hours –is that substantial? Is it about duration, number of users impacted and geography? Are there other factors?

What is meant by "the potential to affect"? Either an incident affects or it does not affect persons.

What is meant by "considerable losses"? 'considerable' is a subjective term and can be interpreted very differently, depending on context. A loss is considerable to the person impacted but may not be considerable to the essential or important entity.

Why are the adjectives 'material' and 'non-material' used at all? Is this a drafting oversight?

20.4

a Why is 'without undue delay' included if 24 hours is objective for initial alerts? Why is there a comment on whether the matter is malicious or not? It may not be possible to have such a definitive position within the 24 hour timeframe. One may suspect and have a high degree of confidence that the incident is malicious or non malicious but it is doubtful that a definitive assessment can be made in advance of the root cause analysis. Is this requirement not premature?

What does "having become aware of the incident" mean? If an incident happens out of office hours, can an essential or important entity not argue that it does not become aware until the start of the following working day on the basis of 'awareness'?

b What would the intermediate report on relevant status updates cover?

c What is the reasoning behind the 1 month timescale for a complete final report? Can the Commission facilitate a sample completed final report, if necessary with the assistance of ENISA so we have a concrete understanding of i), ii) and iii)? What level of granularity is required?

What is meant by "in duly justified cases"? What level or extent of deviation is anticipated?

It is noted that the notification itself does not provide information to ascertain a cross-border aspect to an incident.

20.5

What is meant by 'initial feedback'? Could this be merely an acknowledgement of receipt? It is noted that guidance on the implementation of possible mitigation measures are only to be provided upon request. What about discretion to proactively offer guidance? What precisely is meant by 'guidance'? Is it best practices of a generic nature or is it bespoke specific advice unique to the circumstances of the particular incident? What about liability implications arising following advice from a competent authority or CSIRT?

What is meant by 'additional technical support' and the liability implications arising since CSIRTs don't operate the ICT infrastructure of essential or important entities?

What is meant by providing 'guidance on reporting the incident to law enforcement authorities'? Is this about good digital forensics practises to preserve evidence or mere signposting to relevant law enforcement organisation?

20.6

What role is ENISA to play regarding incidents involving 2 or more Member States? Is there not an obligation on ENISA as well as the Member State authorities to protect the entity's security and commercial interests and confidentiality of information provided? What does ENISA do with this information?

How should such assurance on protection of confidentiality be realised?

20.7

Who determines whether public awareness is necessary? Which Member State takes the lead role? What happens if Member States cannot agree on this matter?

20.9

Why are summary reports required on a monthly basis? What is the reporting now to ENISA rather than to Cooperation Group?

Why is the report about all incidents? How can near misses and significant cyber threats be reported?

What level of aggregation and anonymization is permissible?

Why is there no feedback obligations on ENISA for reports submitted? What is ENISA going to do with this information?

What type of technical guidance is envisaged?

20.10

Why is there an obligation to provide such notification data from NIS competent authorities to CER competent authorities in the absence of a reciprocal obligation on notifications to NIS competent authorities? Why is there no information sharing with NIS authorities? Such information flows may be essential to understanding the full context behind a cyber incident with kinetic effects.

20.11

Why is there no reference to para 4, modalities of notifications and on para 9 on modalities for monthly summary reports with implementing acts?

Article 23

Why is this provision in the proposed Directive? Is this merely about having complete 'WHOIS data'?

23.1

What is meant here by "security, stability and resilience of the DNS"? What is a 'dedicated database facility'? Who are precisely "entities providing domain name registration services"? Registrars?

23.2

What precisely is meant by "relevant information"? Is it names and contact details of points of contact?

23.3.

What type of policies and procedures are envisaged? Are they to be available on a public website? What does publicly available mean?

23.4.

What is 'domain registration data' that is not personal data? Is this role based data on legal persons? Why is the obligation to publish as opposed to facilitate access to legitimate access seekers?

23.5.

Who are 'legitimate access seekers'? CSIRTs? Law enforcement? Others? Why is there no definition in Article 4 for them? What is meant by 'without undue delay'? What type of policies and procedures are envisaged to facilitate legitimate access?

ITALY

Art. 20, par. 2.

Given the broad definition of cyber threats, has the Commission taken in to account the necessity to assure a fair and effective balance between the possible high number of notified threats and the actual capacity of competent authorities or CSIRTS to handle them without being overwhelmed?

Art. 20, par. 3 and 11.

In order to better assess the possible burden on MS deriving from the implementation of the concerned provisions, is the Commission already determined to clarify/specify the notion of "significant" incident in a subsequent implementing act or will such notion be defined by the MS?

In particular:

- par. 3, letter (a)
  - What does the expression substantial "operational disruption" mean and refer to?
  - Does it point to the availability of the service only or include breaches to the integrity and confidentiality of data processed by the ICT system which allows the provision of that service?
  - What does "substantial" mean exactly?
  - Does the Commission plan to establish specific/uniform and binding thresholds to qualify and quantify the "substantiality" of an operational disruption through an implementing act?
  - Does it also plan to do the same with regard to the "substantiality" of financial losses?
- par. 3, letter (b)
  - What does "considerable" material or non-material losses actually mean?
  - Does the Commission plan to establish specific/uniform and binding thresholds to qualify and quantify a "considerable" material or non-material loss through an implementing act or will such thresholds be determined by Member States?

Art. 20, par. 9.

Is there any specific reason why the MS Single Points of Contact are required to submit to ENISA the summary report on incidents, significant cyber threats and near misses on monthly basis? What if the SPoC has nothing to report and submit for a certain month or period?

LATVIA

Article 20

- Paragraph 1: Are there any more specific guidelines regarding reporting process planned (by ENISA or EC)? Are entities those who decide on which recipients in particular case they shall notify? How the information exchange will be coordinated and supervised? Can you provide an example of reporting form (best practice)?
- Paragraph 2: If we use the definition of cyber threats from the REGULATION (EU) 2019/881[3], it's not a good fit here as it covers generic threats as well. Any competent CISO will always have a long list of threats to the information security of his organization. Such a list is the basis for risk management and thus essential for steering defensive measures towards optimal results. It's not something that need to be shared to CSIRTs, competent authorities or recipients of services. What we need here is a different definition. It must be restricted to a concrete event that actually happened. The only thing that can stay in the conjunctive ("might") is the context to an actual outage. In other words, the risk that someone might have compromised the integrity of an organization's network is not worth being reported, but the risk that someone from whom you know is inside your networks will cause a disruption, is. Additionally, we need to make sure that not every entity will need to do a risk disclosure every time a software vendor releases a patch. (Yes, every second Tuesday each month, almost all entities learn about very concrete risks to their infrastructure. Worth reporting? No.)
  In cases, when criteria are general and subject to an interpretation, reporting shouldn't be mandatory and shouldn't include punitive measures. ENISA guidelines, describing cyber threats, thresholds and possible taxonomy could be very beneficial in this regard and worth considering.
- Paragraph 3: Explanation provides room for interpretation. Can it be made more clear/specific? How the "potential" of the incident can be evaluated? Can thresholds for financial loses be established?
- Paragraph 4: Why entities should make a guess if the incident is caused by malicious or unlawful action? What is a purpose of this? It is not clear what the initial notification should contain. For the fulfilment of the obligation set in paragraph 5 (*initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures)*, competent authorities may need appropriate amount of information in this initial notification, what should be reflected in this paragraph.
- Paragraph 5: What happens, if the initial notification is insufficient for CERT to ensure necessary response? What happens response is provided later than in 24h? What is meant by additional technical support? CSIRT may not have necessary technical support or it may be limited.
- Paragraph 6: In the context of ensuring confidentiality – are the networks currently capable to ensure necessary levels of information security? Where these confidential data will be stored and for how long time? Will additional information exchange tools be created or existing enhanced to ensure exchange of classified information?

[3] *"cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.*

- Paragraph 9: What is the purpose of these reports? Taking into account that important incidents should be reported immediately, is there additional benefit of aggregated report? SPOC should not be the ones reporting incidents, as CSIRT is the one who has the necessary information to do that. How would you differentiate cyber threats and near misses? If we are to include near misses, classification of the reports should be elevated.

Article 22

- Paragraph 1: How EC are planning to "*encourage the use of standards*"?

Article 23

- Paragraph 1: Requirement for a "dedicated database facility" is unclear. The term "accurate and complete data" is unclear. If we are to impose these requirements, EC should ensure adequate tools to verify the accuracy of registrant data. Aren't there overlaps with the Union data protection law?
- Paragraph 2: Union data protection law already envisages the obligation to identify the holders of domain names, therefore it is not clear, why such an obligation is set also here.
- Paragraph 3: Can you clarify what is meant by "complete"? What data it would include?
- Paragraph 5: We have a concerns that this may overlap with the existing regulation like Data protection law, E-evidence regulation, Digital service act and CPC regulation. What is the intent to include this in NIS2? What is understood with term "undue delay"?

LITHUANIA

Disclaimer:

The following questions in relation to Articles 20, 22 and 23 of the Proposal are non-exhaustive and might further be expanded.

Although current discussion is solely dedicated to the aforementioned Articles, certain sections of the Proposal were added to Lithuania's comments for the sake of clarity and holistic view of the provisions.

Points of clarification:

Article 20.1:
Could you clarify, when it should be considered that it is "appropriate" for entities to notify the recipients of their services?

Article 20.2:
How should reporting of significant threats by entities should be ensured by Member States? Should the notification of significant threats be conducted also in accordance of para 4 of the Article?

Article 20.2:
Could you clarify when it should be "applicable" for entities to notify the recipients of their services and what measures or remedies that those recipients can take in response would be considered to be enough?

Article 20.3:
Why the definition of significant incident is proposed to be changed compared to a more clear and quantifiable definition of significant disruptive effect in current Article 6 of current NIS Directive?

Article 20.7:
In what circumstances would be appropriate for competent authorities/ CSIRT to notify the public considering the requirement for entities to inform the recipients of their services of significant incidents, according to para 1, and of significant cyber threats, where applicable, according to para 2?

Article 20.9:
Where shall the SPOC have data on near misses if entities are not required to report them to competent authorities/ CSIRT?

Comments in relation to eIDAS:

Since the eIDAS Regulation entered into force, we have perceived the envisaged harmonisation of trust services as well as their general acceptance all over the EU which shows a high success of eIDAS regulation parts related to Trust Services. Thus, any further changes of the existent system should be made, only if needed, thoughtfully and with great caution in order not to jeopardise the success made so far.

The first draft of NIS2 directive foresees to remove Article 19 from the eIDAS regulation with the intention to cover it with NIS 2 directive.
In the area of Trust Services, since the adoption of Directive 1999/93/EC, a customized supervisory system has been established which, among other things, already covers the essential aspects of NIS 2, thus it would be highly important not to jeopardise trust services market and maintain the current system due to its superior level of maturity. It would only suffice to define how eIDAS supervisory bodies cooperate with NIS supervisory bodies.
However, even if Article 19 was still removed from eIDAS regulation, it would be necessary to ensure full alignment of NIS 2 directive and eIDAS regulation (e.g., like it is done with the financial sector) to ensure that such changes would not lead to lower reliability of trust services and less harmonized supervision.

Below are 5 critical issues which should be considered and addressed:

1) Harmonisation of activities/responsibilities between eIDAS supervisory bodies and NIS supervisory bodies. Below are some sample issues we see with current text of NIS 2:

a) It is not clear whether NIS supervisory body will be involved in the process of granting/withdrawing qualified status and if yes, on what level. This is important because aspects, currently covered by Article 19 of eIDAS regulation, affect decision on granting/withdrawing qualified status as security of these services is critically important.

b) It is not clear whether eIDAS supervisory body will get information about incidents and measures that were taken to avoid them in the future. Firstly, this information might affect qualified status of trust service provider (for example, in the case of critical security vulnerability) and secondly, it would be unacceptable if body responsible for the supervision of trust services will not know when trust services are not accessible to customers (in case incident will lead to loss of availability of services).

2) eIDAS regulation focuses on Trust services and its Article 19 encompass security requirements and measures to manage risk posed to Trust services, however NIS2 directive is dedicated only for Network and Information systems. Due to different scopes of these documents, it is highly possible that issues related to security of trust services and not related to network and information systems (e.g., security of customer identification process) will be missed.

3) Article 19 of eIDAS is tightly related to other articles (e.g., Article 13, Article 24). If Article 19 is removed from eIDAS regulation without clearly defining which aspects fall under NIS2 and which under eIDAS, it is likely that some issues (e.g., related to security of QSCDs) will be left uncovered at all (especially high risk as NIS2 is Directive).

4) If eIDAS Article 19 is removed, conformity assessment, currently defined within eIDAS Article 20 and Article 21, will not cover security aspects at all. In such case supervisory bodies might be forced to decide whether to grant/withdrawn qualified status without assessing overall security of these services.

5) Above mentioned aspects should be defined in European level legislation in order not to lower the level of harmonisation. Decrease of the level of harmonisation could occur due to different interpretations in national legislations. Currently this harmonisation of trust services market is very high, and it would be a backward step regressing to the harmonisation level which we had with Electronic Signature Directive.

LUXEMBOURG

Article 20.2

When is a threat considered to be a significant cyber threat? Notion of "could have potentially resulted in a significant incident" is not clear to Luxembourg. Can the Commission explain how this could be determined? Does the Commission plan to include details of a significant cyber threat in the implementing act "to further specify the cases in which an incident shall be considered significant" described in Article 20.11?

Can the Commission explain when a notification to recipients could be applicable and when not, in order to understand the context of this part "Where appropriate, the entities shall also notify those recipients of the threat itself"?

Article 20.3

Can the Commission explain the rationale behind making the description of a "significant incident" less detailed?

Article 23

Does the Commission have plans to make an EU regulation for the database of DNS and TLD registries, considering that the Commission previously also published EU regulation (2018/151) on the security obligations for DSPs?

NETHERLANDS

Disclaimer: The Netherlands is still carefully studying the NIS 2 proposal and is in the process of establishing its position on the content of the proposal. The below list of comments and questions about the proposal is preliminary and may be expanded in the future.

Article 20

General questions and comments:

- Although The Netherlands understands the need for further harmonization of the notification requirements, Member States should be able to further define the parameters for notification in order to take into account national or sectoral circumstances.
- The proposal includes a significant extension of the notification requirements, requiring entities to notify threats and imposing the responsibility to inform recipients of the service. The Netherlands would welcome a further assessment of the consequences of this proposal on the administrative burden for entities within the scope of this Directive.
- As notifications can include sensitive information, the confidentiality of this information must be a crucial prerequisite in setting up mechanisms for exchanging this information between Member States and EU institutions.
- The article differentiates between significant cyber incidents (art. 20, section 1) and cyber threats (art. 20, section 2), but in sections 3-5, the response to cyber threats is omitted. Could the Commission clarify if this is a deliberate choice, and if so, why?

Specific questions:

- Art. 20 (1): Could the Commission clarify the type and scope of incidents to be notified referred to in paragraph 1, especially in comparison with the notification requirements from EECC and eIDAS?
- Art 20 (1): Could the Commission clarify whether the obligation to notify for entities mentioned in art 24 (1) has to be limited to one notification to the single competent authority that has jurisdiction?
- Art. 20 (2): In current legislation, the Netherlands already has a provision that requires entities to notify breaches of their systems that could have a significant impact on the delivery of their service. Could the Commission clarify why it has chosen for the wording ‘potentially have resulted in an incident’ instead of ‘could potentially result in an incident’? The term ‘near misses’ (art. 20 (9)) might not be suitable for threats that still have the potential to result in an incident.
- Art. 20 (1), (2): Could the Commission clarify the difference between “appropriate” in art. 20 (1) and “applicable” in 20 (2)?

- Art. 20 (3): Compared to the current NIS Directive, the parameters that are currently to be taken into account when determining the significance of the impact of an incident have been deleted. What does the Commission consider to be "substantial operational disruption" and "considerable … losses". Would this be left to Member States to decide?
- Art. 20 (5): Could the Commission clarify whether this obligation to respond to the notifying entity would also imposed on competent authorities in the Member States other than the one where the main establishment (art. 24) is established?
- Art. 20 (5): Does this obligation also apply to cyber threats that are suspected to be of a criminal nature?
- Art. 20 (6): Could the Commission clarify what the role of ENISA would be during an incident notification?
- Art. 20 (9): Could the Commission clarify what the objective is of reporting a monthly overview of incidents to ENISA, compared to the annual overview under the current Directive?
- Art 20 (11): According to our initial legal analysis, the authority to adopt implementing acts "further specifying the type of information, the format and the procedure of a notification" would qualify as an essential element of this Directive and, as a consequence, not suitable for implementation through implementing acts.

Article 22

- Art. 22 (1): Could the Commission clarify what 'European or internationally accepted standards' refers to, as mentioned in this article? What process is to be followed to determine this 'status', and who will participate in this process (standards bodies, Member States, ENISA?)
- Art. 22 (1): Could the Commission clarify the term 'encourage'? In what way are Member States obliged to encourage the use of European of internationally accepted standards.
- Art 22 (2): Could the Commission elaborate on what is meant by "advice and guidelines", who this will be given to, to what end, and what the (legal) status of these guidelines will be? What is meant by "'technical areas"? Would this prevent Member States from determining what standards are used in network- and information systems?

Article 23

- Art. 23: Is there any difference between a TLD registry (= term used in this article) and a TLD name registry (= term used throughout the document)? It would appear that they are the same thing, and that the use of two distinct terms is unintended.

- Art.23 (1): Could the Commission clarify the obligation to store TLD data in ‘a dedicated database facility’ given the IT developments like virtualization (separated from hardware) and cloud services?
- Art. 23 (3): Could the Commission clarify which parties are identified as “legitimate access seekers”? Who would decide which organisations or authorities fall under this description?
- Art. 23 (3): Could the Commission clarify whether this includes measures against DNS cache poisoning attacks?

SPAIN

Article 20 Reporting obligations	• This article needs a complete redraft, as it risks harming severely the whole Directive. The current draft does not seem aware that it is stating the terms of administrative sanctioning procedures. And it copies terms from legislations that handle very different contexts, like the Critical Infrastructure legislation. These are very dangerous defects that has been a considerable hindrance to supervisory bodies in the current NIS Directive. In every legislation, behaviors and facts that are to be sanctioned must have at least two or three characteristics. The first characteristic is that these behaviors and facts must be objectively stated and clearly defined. The second characteristic is that these behaviors and facts must be public, knowable, ascertainable to the sanctioner. And proveable. A third characteristic, applicable to this Directive, is that these behaviors and facts must be knowable very early and very easily. The first day. At best, during the first minutes. If the definition is fuzzy or subjective, the sanctioned entities will challenge all sanctions legally with success. If only the entity to be sanctioned knows the fact that it should be sanctioned, and none else in the world can know, or prove, that a sanctionable event has taken place, then the sanctioner (the Supervisory Body) is given an impossible task. If the facts leading to sanction are only knowable (and thus notifiable) weeks or months later then the ciberincident will have gone cold and all notifications, investigations and CSIRT aid will be useless. Same applies if the threshold entails calculating metrics like economic costs to others, that entities very rarely if ever calculate themselves in cyberincidents and never make public. Particularly if they could lead to legal liability. • More clarification is needed about the relation of the proposal with reporting tools as the national security frameworks that Member States may already have in place. • Another issue is that throughout this article “competent authority or CSIRT” is used ambivalently. In accordance with current Spanish legislation that developed the NIS 1 Directive, it is considered a better approach that these functions should be developed by the competent authority, through the CSIRTs, or by the competent authority exclusively according to the case: - **Art 20.1:** - ~~... "to the competent authorities or the CSIRT" ...~~ → ... "to the competent authority, through the CSIRT" ...

	- ~~... "to the competent authorities or the CSIRT" ...~~ → ... "to the competent authority" ...
	- **Art 20.2:**
	- ~~... "to the competent authorities or the CSIRT" ...~~ → ... "to the competent authority, through the CSIRT" ...
	- **Art. 20.3 a)**
	- ~~…"~~ ~~potential to cause substantial operational disruption"…~~ →… " potential to cause serious operational disruption"…
	- **Art. 20.3 b)**
	- ... " ~~causing considerable material~~ " ... → ... "cause serious material " ...
	- **Art 20.4:**
	- ... "~~to the competent authorities or the CSIRT~~" ... → ... "to the competent authority, through the CSIRT" ...
	- … "A competent authority or a CSIRT"… → in this case both would be maintained.
	- … "~~With the competent authorities or the CSIRT~~"… →… "with the competent authority"…
	- **Art 20.5:** When the criminal nature of an incident is suspected, the competent authority (not the CSIRT) does not merely provide "guidance", but rather "issue instructions" for reporting purposes:
	  - ... " ~~Where the CSIRT did not receive the notification~~ " ... → ... "Where the competent authority did not receive the notification " ...
	- … "~~The competent national authorities or the CSIRT will also provide guidance~~"… →… "the competent national authority will provide instructions"…
	- **Art. 20.6:**
	- ... "~~The competent authority or the CSIRT~~" ... → ... "the competent authority" ...
	- **Art 20.7:**
	- … "~~The competent authority or the CSIRT and, where appropriate, the authorities or CSIRT of~~"… →
	- ... "The competent authority and, where appropriate, the authorities of" ...
	- **Art 20.8:**
	- ... " ~~of the competent authority or the CSIRT~~ " ... → ... " of the competent authority or the CSIRT " ...
	
	• The impact on the CSIRT may be high due to the increase in the number of entities under NIS2, and the establishment of response obligations in very short periods, this will increase costs beyond what is foreseen by the COM.
	
	• Article 20.2 states "2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident".
	  ○ How can Supervisory Bodies know what threats the entities have suffered, without spying in on them?

	○ How can Supervisory Bodies know what threats the entities have identified? ○ How can Supervisory Bodies know that a particular threat could have potentially resulted in a significant incident, and what would this mean in an objective definition? In practice, the metrics and thresholds Supervisory Bodies can know from public sources are very different. I.e. duration of the incident in days. Also, the article includes the terms "where applicable", "where appropiate", etc. This leaves a large berth to national transpositions of the Directive, which will lead to a heterogeneous NIS legislation. • Article 20 states "3. An incident shall be considered significant if: (a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned; (b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses." These terms make sense in the case of incidents in the physical world, where material or non-material losses are public and knowable, if only approximately. In the case of cyberattacks they do not make sense, as the only public source of information are the attacked entities' press releases. - How can Supervisory Bodies know what operational disruption, material and non material losses the entities or third actors have suffered? - How can Supervisory Bodies know if a supervised entity has not complied with this Article? - How can Supervisory Bodies prove that a non-notified incident has been significative contrary to the attacked entities statements, if the only public source of information are the attacked entities' press releases? - How can an attacked entity (or the Supervisory Body) know that a particular threat has the potential to cause a certain amount of losses? Some entities receive hundreds of threats a day (phishing spam, botnets, etc.), most with a very low probability of succeeding but a high damage if they succeed. - Incidents often continue adding up material costs during weeks or months, and this duration is difficult to gauge. How can we expect early warnings and notifications of incidents if we impose an economic calculation as a metric?

	• A more detailed definition of the incidents should be included. We have neither taxonomy nor criticality criteria. On the other hand, the concept near misses is not understood. It is an incident under investigation that when it ends could end in a false positive? A good practice provided by ENISA is necessary to establish the **taxonomy and criticality including transnational notification criteria**. Spain believes **that incident classification** should be based on **potential impact and hazard level** and supports ENISA's incident taxonomy. On a separate issue, initial incident notification and incident management notification are also aspects to be considered in the review. This classification is considered ambiguous. It is requested that clarify what a significant incident is. In Spain we have considered incidents of criticality / dangerousness as HIGH, VERY HIGH and CRITICAL. Creation of a one-stop-shop method for cybersecurity notifications in Europe. This mechanism would help to share information among all the interested entities. These notifications should be considered as a minimum requirement and it should be established in the NIS 2.0 Directive that Member States should promote common notification platforms to speed up this notification at the European level. Regarding incident management, special attention should be paid to foster implementation of common metrics, thresholds and scales to categorize incidents. It is required to define thresholds and metrics, easy to measure and cost-effective, more suitable for determining the significance of the impact of an incident in the continuity of services. • Finally, in art. 20.5 when the criminal nature of an incident is suspected, the competent authority (not the CSIRT) does not merely provide "guidance", but rather "issue instructions" for reporting purposes.
Article 22 Standardisation	There is a mention to coordination between ENISA and "Member States". This is not enough. Two more coordinations should be explicitly mentioned: direct coordination of ENISA with the national Member States' standardization bodies and direct coordination of ENISA with the european and international standardization bodies. This should be fostered in order to facilitate the promotion and effective applicability of European standards.

SWEDEN

Article 20

Article 20 is in general comprehensive and detailed. SE would like the Commission to clarify if the Member States, pursuant to Article 3, may go beyond what is stated in Article 20. If this is correct, does the Commission consider that there is a risk for continued fragmentation within the EU regarding these issues?

SE would prefer a more general writing in Article 20, which would leave room for Member States to work on the basis on their own preconditions and needs. What does the Commission consider to be added value of the Member States reporting the same data? Is the purpose of this to have comparable data at EU level?

Article 20 (2)

Could the Commission please clarify how this paragraph would be implemented in practice. For instance what is meant by ”without undue delay” and how would competent authorities or the CSIRT decided when the requirements are met? Or would it be up the Member States to develop regulations regarding this issue on a national level?

Article 20 (3)

The meaning of a significant incident needs to be further clarified in order for Member States to be able to comprehend and incorporate the proposal in a harmonized way. In particular the meaning of wording “potential to cause substantial operational disruption”.

We would also appreciate if the Commission could further elaborate over any secondary or cascading effects due to incidents and how to more effectively cover these in the definitions of ”significance”.

Article 20 (5)

In Article 20 (5) it is stated that the competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. SE would like the Commission to clarify what is mean by “initial feedback on the incident” and also elaborate on the added value by doing this?

Article 20 (9)

At present, the single point of contact, submits an annual report. In the proposal it is stated that a summary report, including anonymised and aggregated data on incidents shall be submitted to ENISA on a monthly basis. SE would like the Commission to elaborate on the purpose of this and also clarify what “near misses” means and why ENISA needs this information. How will this work in practice and is this justified in view of increased workload for the single point of contact?

Article 20 (10)

It would be appreciated if the Commission could develop and clarify the relation between CER (Directive on Critical Entities Resilience) and NIS2 in this Article. What is the purpose of the information sharing and would all incident reports linked to the essential entities be shared with CER or will the monthly reports be shared with CER?

Article 20 (11)

SE has some concerns that the implementing acts, as stated in Article 20 (11) will affect the ability of the Member States to work on the basis on their own preconditions. Implementing acts can have a major impact on the Member States which already have come a long way in their work with, for example, reporting obligations as stated in this Article. Implementing acts could overthrow the work in progress and lead to increased costs for the Member States. Could the Commission elaborate on this and the added value of adopting implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2.

Article (23)

SE would like the Commission to elaborate on the purpose of having regulation at such a detailed level regarding the issue of databases of domain names and registration data?