

## Table of Contents

AUSTRIA .....	1
BELGIUM .....	5
CZECH REPUBLIC .....	9
DENMARK .....	13
FRANCE .....	16
GERMANY .....	60
HUNGARY .....	71
IRELAND .....	90
ITALY .....	117
NETHERLANDS .....	142
SPAIN .....	161
SWEDEN .....	186

## AUSTRIA

Horizontal Working Party on Cyber Issues – Drafting COM(2020) 823 final (NIS2)


### Comments and drafting proposals by Austria

23.06.2021

**Remark: The comments by Austria focus on issues that we consider as predominantly important. The comments are not exhaustive and we reserve the right to make further comments in due course.**

NIS2 reference	Comments	Drafting proposal
Article 17 Para. 1a	<ul style="list-style-type: none"><li>There should be a duty to report to the management body to facilitate the task of supervision. The current text gives too much leeway as to what “supervision” encompasses and would not allow to hold management bodies accountable for the non-compliance.</li></ul>	<ul style="list-style-type: none"><li>Add new para 1a: “For the purpose of supervising the implementation of the cybersecurity risk management measures, the management body shall receive a quarterly report on the current status of their implementation.”</li></ul>
Article 18 Para. 1	<ul style="list-style-type: none"><li><b>BJA:</b> We suggest to delete the phrase “which those entities use in the provision of their services” since it is unclear what type of services are meant. It seems to be a reminiscence of the concept of essential services.</li></ul>	<ul style="list-style-type: none"><li>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 and information systems <del>which those entities use in the provision of their services.</del></li></ul>

NIS2 reference	Comments	Drafting proposal
Article 18 Para. 2 lit. f	<ul style="list-style-type: none"> <li>It remains unclear, if “testing and auditing” would require third party auditing or if it would be possible to have self-assessments and self-tests as well. We do not think that it is necessary to specify this here. It could be mentioned as an example in a recital.</li> </ul>	<ul style="list-style-type: none"> <li>policies and procedures <del>(testing and auditing)</del> to assess the effectiveness of cybersecurity risk management measures;</li> </ul>
Article 18 Para. 4	<ul style="list-style-type: none"> <li><b>BJA:</b> The term “tasks” only appears here. Moreover, it is unclear what type of services are meant. Furthermore, service is not what should be compliant but the security measures in paras 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Member States shall ensure that where an entity finds that it is <del>respectively its services or tasks are</del> not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring <del>it the service concerned</del> into compliance.</li> </ul>
Article 19 Para. 1	<ul style="list-style-type: none"> <li>As Commission and ENISA enjoy full membership in the CG according to Art 12.3 anyway, to mention them explicitly in Art 19 para 1 appears unnecessary.</li> <li>In CSA we usually refer to ICT products, services and processes, the term “systems” is undefined.</li> </ul>	<ul style="list-style-type: none"> <li>The Cooperation Group, <del>in cooperation with the Commission and ENISA,</del> may carry out coordinated security risk assessments of specific critical ICT <del>products, services, systems or processes</del> <b>products</b> supply chains, taking into account technical and, where relevant, non-technical risk factors.</li> </ul>
Art 20	<ul style="list-style-type: none"> <li>We suggest separating the reporting of incidents and the reporting of cyber threats into two different Articles. Furthermore, the reporting to CSIRTs or CAs should be in a separate para than the reporting to recipients since the content and addressees of the notifications are different.</li> </ul>	
Article 20 Para. 1	<p><b>Sentence 1</b></p> <ul style="list-style-type: none"> <li>While sentence 1 mentions “without undue delay” like in para 4, it does not do so for “in any event within 24 hours”. Thus, we suggest to include the time limit already in sentence 1 (also, we think 24 hours is too long).</li> </ul> <p><b>Sentence 2</b></p> <ul style="list-style-type: none"> <li>The qualifier "when appropriate" is crucial to make this</li> </ul>	<ul style="list-style-type: none"> <li>Member States shall ensure that essential and important entities notify, without undue delay <b>and in any event within 12 hours</b>, 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.</li> </ul>

NIS2 reference	Comments	Drafting proposal
	<p>workable. Determining the "recipients of their services" is in many cases "whoever might walk through our door tomorrow" (e.g. with regard to supermarkets or hospitals). It may in many cases be not possible to do targeted notifications, which leads to the question how those cases should be handled. Thus, it is key to determine when such a case would be appropriate (e.g. by listing examples in a recital) and how the notification should take place (e.g. direct notification or statement on website or social media)</p> <ul style="list-style-type: none"> <li>• The provision should not lead to a heavy administrative burden for entities</li> <li>• Since sentence 2, compared to sentence 1, regulates a different kind of reporting duty (different recipients, different content), we suggest to create an own para for it.</li> </ul>	
Article 20 Para. 2 Subpara 1	<ul style="list-style-type: none"> <li>• The definition of "cyber threat" in the Cybersecurity Act (2019/881) means any potential circumstance, event or action that could damage, disrupt or otherwise adversely affect network and information systems, the users of such systems and other persons. This definition is quite broad. The link to a potential significant incident is needed, but could benefit from further specification. It should be elaborated (e.g. in a recital) that para 2 should capture events like cyberespionage, APT or the risk that a malicious threat actor is known to be inside the networks and has the means to cause a disruption. 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.</li> </ul>	
Article 20 Para. 2 Subpara 2	<ul style="list-style-type: none"> <li>• It should be elaborated in a recital that it is not appropriate to notify the recipients of the threat when this would decrease the level of cybersecurity of the entity or increase its level of exposure to the threat.</li> </ul>	

NIS2 reference	Comments	Drafting proposal
Article 20 Para. 4a	<ul style="list-style-type: none"> <li>We deem 24 hours too long.</li> </ul>	<ul style="list-style-type: none"> <li>"... without undue delay <b>and in any event within 12 hours</b> after..."</li> </ul>

## General orientations from BELGIUM concerning Articles 2, 17-22, 28-33 as well as the Annexes of the Commission's proposal for the NIS2 Directive

Belgium welcomes the incoming Slovenian Presidency's determination to make swift progress in the negotiations with a view to achieving a general approach for a new Directive on measures for a high common level of cybersecurity across the Union (NIS2).

In the past, Belgium has voiced its support for the overall objective of the Commission's proposal to bring about more clarity and harmonization in the current legislative framework where needed. In light of the ever increasing threat landscape, it is imperative that we adapt the NIS framework to the reality of today, while also rendering it future-proof. Belgium will therefore continue to work constructively with the upcoming Presidency and other Member States in the Council on this file, which is of considerable importance to our economies and societies.

Following the request of the incoming Presidency, Belgium would like to share the following **general orientations** with regards to Articles 2, 17-22, 28-33 as well as the Annexes of the Commission's proposal for the NIS2 Directive. It is important to note however, that these **orientations are not exhaustive and do not prejudice any future positioning**. Within the short timeframe put forward by the incoming Presidency, it was not feasible to work through the regular interdepartmental coordination process, necessary for compiling substantial written comments.

### 1. Scope

With article 2(1), the Commission has opted to abandon the current philosophy of NIS1 – which applied to entities identified by Member States – in favour of a size criterium (the size-cap). The Commission's proposal would now oblige all entities in the listed sectors, with the exception of micro and small enterprises, to adhere to cybersecurity risk management requirements and reporting obligations.

There are a few drawbacks to be raised with regards to the size cap, which Belgium hopes to address during the upcoming negotiations on the scope. Notably a) the apparent absence of the element of risk, b) the difficulty in prioritizing supervision or assistance, c) the lack of proportionality, especially with regard to SMEs, d) consideration of national public organisational structures and e) the loss of overview for supervising authorities.

#### a) Risk based approach

While the size-cap offers the important advantage of a clear and immediate identification criterium, the sole element of size does not seem to take the actual criticality of an entity sufficiently into account. **Belgium would welcome all initiatives from Member States that aim to further emphasize a risk based approach, allowing for diversification in identification, security requirements, supervision and/or enforcement.**

#### b) Prioritization of supervision and assistance

While the proposed enlargement of the scope will broaden the set and number of entities that should take appropriate measures and notify incidents, the current proposal of dividing these entities into important versus essential entities based solely on the sector they operate in will make it more difficult for authorities to prioritize their supervision or for CSIRT to prioritize their assistance to entities. Within each sector all of the entities in scope would be considered equally 'essential' or important, while it is clear that some entities in each sector deliver more or more significant essential services, as indeed the NIS1 approach suggested. In particular for some subsectors in the digital infrastructure sector, the current provisions would even mean that all entities operating within that same sector would be deemed

equally essential. Belgium would therefore welcome all initiatives from Member States that introduce elements allowing for a more layered consideration of entities, also within sectors.

c) Proportionality

Additionally, Belgian administrations as well as business communities are concerned by the risk of overburdening medium-sized companies (50-250 FTE or >10 M€ turnover) and supervisory authorities if the scope would be enlarged in the proposed manner. As a result, resources as well as focus might be lost.

European SME's are at the forefront of digital innovation and face cyber threats on a regular basis. Belgium prefers to prioritise a 'get the basics right' approach, providing adequate assistance, leveraging investment and stimulating SME's to build capacities and raise their resilience. By contrast, overwhelming medium-sized enterprises with burdensome regulation and complex requirements should not be the first answer. Unlike their large peers, many medium-sized enterprises have not been confronted before with similar requirements and start off with a disadvantage to reach compliance.

According to the Commission's own estimates, the current size threshold would result in a more than 600% increase of the number of entities subject to supervision. It goes without saying that supervisory authorities under this Directive would be overwhelmed with cyber incident and threat notifications from a multitude of entities without a demonstrable critical nature.

Therefore, if the approach of a size criterium were to be pursued, Belgium emphasizes that it should be left to Member States to identify micro, small and medium-sized enterprises which are of vital importance for key societal and economic activities. In consequence, the identification mechanism foreseen in article 2(2) could be expanded to medium-sized enterprises. This would effectively prevent entities that are of actual critical importance from falling out of the scope all together. The influx of incident and threat reporting would be limited to workable levels for supervisory authorities to handle.

Belgium is convinced that such an approach will generate more goodwill and initiative from within the SME community, hence enable to achieve higher levels of cyber threat awareness and cyber security.

*Article 2*  
*Scope*

1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro ~~and~~, small **and medium-sized** enterprises within the meaning of Commission Recommendation 2003/361/EC.

d) Public administrations

Public administrations deliver essential services to its citizens each day. Recent attacks have shown, however, that they are also a target for malicious cyber activities. It is therefore imperative that public administrations take all necessary measures to safeguard the availability, integrity and confidentiality of their networks (as well as the data they hold of citizens and public servants).

Belgium considers it highly important that public administrations are a part of the scope of the NIS2 Directive. It serves as an additional driver for increased cybersecurity efforts on the part of public authorities, as well as an important signal to the public and the private sector within and outside of the Union that public administrations are set to do their part.

However, while Belgium agrees that public administrations should be included in principle, it believes Member States should retain the full responsibility and flexibility to lay down the rules governing public administrations with regards to identifying which entities are in scope, as well as their security measures, reporting obligations, supervision and enforcement. Such an approach will allow Member States to take into account the specificities of national organizational structures and territorial subdivisions.

In order to lay out the reasoning and suggested text amendments, Belgium has co-sponsored a **non-paper on the inclusion of public administration in the NIS2 Directive framework**, together with PL, DE, HU, IT, MT, NL and SE.

e) Registration of entities

With the absence of an identification mechanism, supervisory authorities lack a clear picture of the entities that automatically fall under their jurisdiction. A similar shortcoming was identified in the supervisory framework of Digital Service Providers (DSP's) in the current NIS Directive. Sending targeted warnings to essential entities about cybersecurity vulnerabilities is a strategic priority for Belgium, and indeed an important task for CSIRTs in the entire Union, as stressed in this Directive (Art. 10(2)b). In order to do so, CSIRTs need to have contact points to quickly and directly warn these entities. In order to perform supervisory and enforcement activities, as well as to deliver assistance and other CSIRT services like 'spear warning', **Belgium sees the important need for a national registration mechanism which lists the entities concerned by this Directive and which provides authorities with a contact point for each entity.** Entities should be required to register themselves at their national authority and/or CSIRT. For reasons of clarity and harmonization, this mechanism should be inscribed in the operative part of the Directive.

## 2. Cybersecurity risk management and reporting

Belgium welcomes in principle the increased clarity and harmonization that comes with articles 17 to 22 of the Commission's proposal as compared to the current NIS Directive. These strengthened provisions will in particular serve entities and sectors which maintain cross-border activities throughout the internal market, as well as the efficient coordination between supervisory authorities.

a) Security requirements

Requiring entities to take a set of minimum cybersecurity risk management measures is a crucial element of this Directive. Belgium welcomes the objective of increased harmonization in this regard. It would be opportune, however, to hold a thorough discussion on each proposed minimal measure in order to evaluate its appropriateness and feasibility.

Sufficient attention should in this regard be given to the security of supply chains. Part of the responsibility in the management of supply chain risks lies with the entities themselves. However, in reality it is not always possible for entities to negotiate stricter terms with larger or historical suppliers, providers or vendors. **The possibility of establishing a direct link with these suppliers and extending responsibilities through the NIS2 Directive should therefore be explored.**

b) Reporting obligations

Belgium underscores the importance of receiving incident notification in the shortest possible delay, without this resulting in an unreasonable burden for operators in the course of a cyber incident. **Belgium therefore requests to delete the 24 hour deadline for initial notifications in the current Commission's proposal.** The proposed 24 hour timeframe is not suitable for all of the sectors in the

scope of this Directive. **Belgium insists that the wording in the current NIS Directive of “without undue delay” is to be maintained**, with the possibility of further refining this timeframe in light of sectoral specificities.

The thresholds for assessing the significance of an incident should be further elaborated in the Directive to provide maximum clarity.

Belgium supports the Commission’s proposal to require entities to not only report cyber incidents, but also cyber threats that could have potentially resulted in a significant incident. The Belgian experience with regards to ‘Spear Warning’ shows that informing the recipients of the services of potential threats in a targeted manner, combined with possible actions they might take, increases trust and the overall level of security. The concept of near misses, on the other hand, deserves further clarification.

The submission of a summary report, including anonymized and aggregated data on incidents, threats and near misses to ENISA should be limited to a quarterly exercise. Monthly reporting would result in less solid and less comparable statistics, as well as an overburdening of national authorities.

Belgium would like to express caution as to further specifying the type of information, the format and the procedure of notifications by means of implementing acts. Any future modification should take into account and not be incompatible with established practices at national level. Nor should it impede the complementarity that this Directive intends to foster between reporting obligations and notification templates under the frameworks of NIS and other related or sectoral legislation.

### **3. Supervision and enforcement**

Belgium welcomes the increased attention on effective supervision over entities in the scope of this Directive. It supports the general objective of reinforcing the toolbox of supervisory authorities for them to be sufficiently equipped to monitor compliance.

Nonetheless, **Belgium advises caution with regards to the punitive aspects of the enforcement toolbox**. The use of punitive measures, including administrative fines, must never be a goal in itself. Additionally, severe action must be exclusively reserved for exceptional cases of ultimate necessity. **In order to be an effective stimulus for compliance, the threat of punitive measures must be proportionate and thus credible**. Punitive action may never constitute an additional hindrance for entities to adopt protective measures. Belgium looks forward to addressing these concerns during upcoming negotiations over articles 28-33.

In this light, **Belgium tends to reject the proposed public disclosure and liability frameworks concerning natural persons** in article 29. To raise the overall cybersecurity of an entity, it is indeed necessary to sufficiently implicate the managerial level. Nonetheless, trust between managers and security officers is even more crucial in order to make progress. Publicizing certain information could at the same time improve transparency, as well as expose society and entities to supplementary threats. Due restraint should therefore be exercised with regards to these regulatory changes.

## CZECH REPUBLIC

CZ comments on NIS2 (Art. 2, Annexes, Art. 17-22, 28-33)

### Scope – Art. 2 and Annexes

#### **The size-cap rule**

Unfortunately, the size-cap rule does not properly reflect the importance of entities to the Member States and the whole Internal Market from the security perspective. Therefore, the application of this rule as a sole criterion for the identification of all entities under the NIS2 is not proportionate. We consider the usage of this rule problematic because we think that to really increase the overall level of cyber resilience throughout the Internal Market the most crucial entities falling in the scope of the NIS2 should not just be regulated but also proactively supported by national competent authorities and provided with enhanced services by CSIRTs. Unfortunately, the size-cap rule does not allow for such a tailored and proportioned approach. Instead, it suggests targeting and regulating a wide variety of entities of similar size in the same way, without any reflection of their importance for key societal and economic activities within the Internal Market and therefore creating unnecessary and a disproportionate burden for national competent authorities. In addition, the size-cap rule can be misused for purposes of avoiding the cybersecurity regulation by companies deliberately manipulating their organizational structures etc. And conversely, some entities might fall in the scope of the NIS2 only because of being part of a larger corporation. How the size-cap rule should apply in these cases is not clear. Moreover, the size of companies is fluid. That means that some companies finding themselves on the edge of size cap might be repeatedly falling in and out of the NIS2 scope. For these reasons, we would like to open the discussion in the HWPCI in order to find a different way of setting the scope of NIS2 to ensure that the NIS2 Directive would uphold the principles of subsidiarity and proportionality, its scope is well-targeted and meets its aim to enhance the cybersecurity across the Union.

#### **Self-identification**

Should an EU uniform identification criterion be preserved in the final version of the NIS2, we think that it is absolutely necessary to ensure that the self-identified entities report themselves to the national competent authorities. Without a self-reporting mechanism, we risk that the national competent authorities lose the awareness about entities that are regulated in their national legislation which would limit their knowledge about them and the environment as a whole where they should perform their tasks. Moreover, the national competent authorities would not be sure which entities fall under the regulation and have to comply with certain cybersecurity requirements. This non-awareness could therefore complicate the execution of their enforcement and supervision tasks. Lastly, in practice it is not always clear what size do companies have in the meaning of the Commission Recommendation 2003/361. The application of size-cap rule without a self-reporting mechanism brings an additional burden for national competent authorities looking for entities to be regulated and assessing their size – which is by no means an easy job. Therefore, the NIS2 should set an obligation or specific procedure to ensure that self-identified entities self-report themselves to the national competent authorities.

#### **Public administration**

We acknowledge that enhancing cybersecurity of public administration (PA) entities is desirable. Nevertheless, legal framework and organization of PA differs considerably among the Member

States. Therefore, setting uniform criteria for the identification of PA entities and obligating them comes with the risk of not targeting the right PA entities and therefore making such approach not proportional. Moreover, the NIS framework would have to include and anticipate many opt-outs and exceptions for PA in the context of their obligations and supervision. Therefore, we propose to stipulate a general obligation for the Member States to regulate their PA entities in their national cybersecurity legislation and leave the PA out of the scope of the NIS2 to let the Member States to choose the proper way (criteria, obligations and supervision regime) to regulate PA entities on the basis of their actual needs. We think that this approach falls best within the subsidiarity and proportionality principles. See the drafting proposal in the Annex of this document.

### **Services vs. entities regulation**

The NIS2 proposes to regulate entities, not services as the NIS1. The Commission justifies this approach with the argument that the enterprise network and systems are interconnected so the regulation of the whole entity make sense. In addition, the entities may decide on what networks and information systems their security measures would focus on the basis of the prior risk analysis. This approach, however, has its drawbacks. Firstly, it may create an additional burden for entities providing various (more or less isolated) services with different security risk levels. And secondly, the regulated entities might identify some systems as priority from their business perspective as such accounting software and give less priority to the systems for which they are actually regulated such as systems related to the distribution of gas.

### **Submission of list of entities to the Commission**

We think that this obligation is redundant with no clear benefit. Any submission of such highly sensitive list to anyone should be left to the decision of Member States.

### **Lex specialis**

We support further specifying the lex specialis provisions in the NIS2, including the idea of baseline requirements.

### **Trainings of management bodies under the Art. 17 para 2**

We support more engagement of management bodies in the regulated entities' cybersecurity risk management. However, we want to point out that some national legislations and/or enterprise-level risk management procedures inspired by widely recognized international standard such as ISO 27K include a special role of chief information security officers (CISOs). Where CISOs were pointed, they would probably participate in cybersecurity trainings and they would surely need to have good knowledge about entity's cybersecurity risks as they would be primarily in charge of managing it. Requiring also other members of management bodies than CISOs to undertake *trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the entity* might be excessive, particularly in the case of small companies where CISOs were appointed.

### **Security measures under the Art. 18**

Coming back to entities vs. services regulation problem outlined above we think that if the obligations were imposed on the entities as whole, complying with the measures under Art. 18 para 2 might be burdensome and possibly mistargeted. We are of a view that the (unquestionably needed) risk-based approach and risk analysis (under Art. 18 para 2 point a) do not themselves guarantee that entities will target the right networks and systems. Clarification in this regard, i.e. specification that the entities shall target the right networks and systems, is needed and shall be added into the NIS2 normative text.

Even with having in mind the risk-based approach, the set of the measures introduced in the Art. 18 para 2 seems to be a very ambitious security baseline for all NIS entities. We think that the application of some measures may turn to be very burdensome. For example, in the context of supply chain security, it is neither proportionate nor efficient to require all NIS entities to deal with all of their suppliers (as supposedly suggested in Art. 18 para 3). For smaller entities, it might be very challenging to apply this measure even when focusing on their most important suppliers, service providers and managed service providers. More strategic, proportionate, risk-based approach must be taken here. Another measure which we think that would be burdensome and disproportionate is the vulnerability disclosure under 18 para 2 point e. While we acknowledge that this measure represents a good practice (as well as CVD under Art. 6), we do not think it is necessary that any NIS entities comply with it on the mandatory basis. Unlike vulnerability handling, it should be purely voluntary practice (the same applies for CVD). Also, the requirement on the use of cryptography and encryption needs to be treated cautiously.

In order to keep the requirements well-balanced and bearable as well as to make the categorization of entities under the NIS meaningful, the Member States should have the last word on the implementation of the requirements (specification of methodology, contextualization, procedures etc) and also be given the opportunity to require stricter requirements for the essential entities. Therefore, we do not support the inclusion of the implementing and delegated acts into this Article which aims to empower the Commission to lay down specification of measures and enlarging the list of measures. We think that this creates legal uncertainty for both regulated entities and national authorities and hampers the two-categories approach. At the same time, we appreciate the work on guidelines, reference documents and other materials undertaken in the framework of the NIS CG which is helpful for finding common understanding, exchange of experience and knowledge building. This practice certainly contributes to increasing the cybersecurity throughout the Union

and it should continue doing so. We also appreciate all the work of ENISA on its supporting materials.

### **Use of cybersecurity certification schemes – Art. 21**

We think that the CSA already provides a good basis for detailing the (obligatory) use of EU cybersecurity certification schemes. Accordingly, we think that this Article is redundant and with no experience with the application of schemes so far also unjustified.

## Supervision

### **Ex-post supervision**

We think that we need further clarification of how the ex-post supervision should work, particularly what are the triggers.

### Annex

Drafting proposal related to the regulation of public administration entities

New paragraph in the Article 2:

Member States shall ensure the network and information systems used by their public administration entities are subject to their national cybersecurity regulation.

New recital 20a:

Where appropriate, public administration entities should be subject to obligations similar to those for essential and important entities.

## DENMARK

Dear Secretariat and Presidency,

Here are the Danish comments and initial drafting proposals on Article 2 and Annexes, and Articles 17-22, 28-33, in the NIS2 Directive.

### Article 2

‘(f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State; *or*’  
(background: adding an “or” would indicate that just one – not all – of the stated conditions would need to apply)

### Article 2, 3. (a)

All issues with respect to member states’ national security must be clearly exempt from NIS2. The proposed wording is insufficient in the regard.

An alternative text in line with the wording of the Council’s proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications art. 2 (2 a) may serve as a model:

*‘2. This Regulation does not apply to:*

*(a) activities, which fall outside the scope of Union law, and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority;’*

Article 2 (5 a):

The text ”including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.” should be softened so that the wording of the article is brought in line with GDPR, art. 32 which merely states: “Taking into account state of the art...”.

Article 2 (2a) (addition of new text)

*‘This Directive does not apply to top-level domain name registries referred to in point 8 of Annex I if the top-level domain name is used by a registry only for own use’*

(background: Some top-level domain names are acquired by owners of brands either for their own use or as a defensive registration. It is not regarded as proportional that such entities are covered by NIS2).

Article 18, 5. and Article 20, 11.

\*5. The Commission ~~may~~ shall adopt implementing acts **by (date to be fixed later)** in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. When preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.’

and

\*11. The Commission ~~may~~ shall adopt implementing acts **by (date to be fixed later)** further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission ~~may~~ shall also adopt implementing acts **by (date to be fixed later)** to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).’

(background: A delayed or failure to adopt implementing acts, as soon as possible after the NIS2 Directive enter into force, may be a cause for doubt, uncertainty and concern for entities, as to which requirements they should live up to. NIS2 should determine a date for adopting implementing acts, in the same way as in the existing NISD regarding the adoption of implementing acts concerning digital services. The experience from NISD with implementing acts for notification of security incidents for digital services also hints, that such notification/threshold limit values should be adapted to each individual sector/service, should be further defined in NIS2).

Art. 29, 4 (j) and Art. 30, 4 (i)

The Commission informed HWPCI on April 19. 2021, that it is being aware of the fact that administrative fines are a constitutional problem for DK. At the meeting the Commission mentioned, that a possible solution could be, to refer to fines without qualifying them as administrative, or by trying to find a special solution for DK, as in the case of GDPR. In this regard, **we would like to suggest that use of the word “administrative”, in references to “administrative fines”, is being stricken** (so that the term used will just be: “fine” or “fines”). Alternatively, DK might see a solution in a wording that could be similar to GDPR article 83, 9 (which may almost be used interchangeably).

Article 32:

**The article should be stricken.**

(background: GDPR art. 33 already contains a requirement of notification of a personal data breach to the supervisory authority be the controller. The NIS competent authority is typically not in a position to file a complete notification to the DPA, a notification which would anyway merely duplicate that of the **controller**.)

**Notwithstanding the foregoing, Denmark takes general scrutiny reservation and parliamentary scrutiny reservation concerning the scope of the NIS2 Directive, and also emphasizes that nothing contained herein shall be deemed or construed as binding, until an official agreement concerning the NIS2 Directive has been reached.**

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**

(Text with EEA relevance)

(...)

HAVE ADOPTED THIS DIRECTIVE:

**CHAPTER I**

*General provisions*

*Article 1*

***Subject matter***

1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.
2. To that end, this Directive:
  - (a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);
  - (b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I and important entities in Annex II;
  - (c) lays down obligations on cybersecurity information sharing.

## Article 2

### Scope

1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.<sup>1</sup>
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;
  - (b) the entity is a public administration entity as defined in point 23 of Article 4;
  - (c) the entity is the sole provider of a service in a Member State;
  - (d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;
  - (e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;
  - (f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;
  - (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council<sup>2</sup> [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.

Member States shall establish a list of entities identified pursuant to points (b) to (f) ~~and submit it to the Commission by [6 months after the transposition deadline]~~. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.

**(New) The entities identified in Annex I and II shall register with the national competent authority by [ X months after the transposition deadline]**

<sup>1</sup> Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

<sup>2</sup> [insert the full title and OJ publication reference when known]

3. This Directive is without prejudice to the **actions taken** ~~competences of~~ **by** Member States and their competences **regarding activities concerning the maintenance of public security**, defence and national security **and the activities of the State in areas of criminal law including the protection of information the disclosure of which Member states consider contrary to the essential interests of their security, in compliance with article 346 TFUE.** ~~compliance with Union law.~~ Thus, public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security shall be excluded of the scope of this Directive.
4. This Directive applies without prejudice to Council Directive 2008/114/EC<sup>3</sup> and Directives 2011/93/EU<sup>4</sup> and 2013/40/EU<sup>5</sup> of the European Parliament and of the Council.
5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.
6. ~~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.~~

## New Article

### Sector-specific Union legal acts

1. **The Commission is empowered to adopt implementing acts when additional sector-specific provisions pertaining to cybersecurity risk management measures and notification obligations appear to be necessary to ensure a high level of cybersecurity,**

---

<sup>3</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

<sup>4</sup> Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

<sup>5</sup> Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

2. In the event that the use of these procedures is not possible, where adopting sector-specific Union legal acts requiring essential or important entities to adopt cybersecurity risk management measures, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, shall not apply to those entities.
3. The Commission and ENISA should regularly assess the application of the equivalent effect requirements in relation to sector-specific provisions of Union legal acts.
4. The Commission, taking duly into account the opinion of the Cooperation Group and with the assistance of ENISA, shall issue guidelines or recommendations on actions or measures to be taken by the sector-specific legislation's competent authorities to ensure that sector-specific legal acts meet the minimum security requirements laid down by the Directive.

### *Article 3*

#### ***Minimum harmonisation***

Without prejudice to their other obligations under Union law, Member States may, in accordance with this Directive, **regulate a broader scope of entities and** adopt or maintain provisions **or** ensuring a higher level of cybersecurity.

### *Article 4*

#### ***Definitions***

For the purposes of this Directive, the following definitions apply:

- (1) 'network and information system' means:
  - (a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;
  - (b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;
  - (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;
- (2) 'security of network, services and information systems' means the ability of network, services and information systems to resist, at a given level of confidence, any event that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network, services and information systems;

- (3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council<sup>6</sup>;
- (4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;
- (5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;
- (6) 'incident handling' means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;
- (7) 'cyber threat' means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881;
- (8) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a cyber threat;
- (9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;
- (10) 'standard' means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council<sup>7</sup>;
- (11) 'technical specification' means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012;
- (12) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;
- (13) 'domain name system (DNS)' means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;
- (14) 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;

---

<sup>6</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p.15).

<sup>7</sup> Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p.12).

- (15) ‘top–level domain name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers;
- (16) ‘digital service’ means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council<sup>8</sup>;
- (17) ‘online marketplace’ means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council<sup>9</sup>;
- (18) ‘online search engine’ means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council<sup>10</sup>;
- (19) ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources;
- (20) ‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;
- (21) ‘content delivery network’ means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;
- (22) ‘social networking services platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);
- (23) ‘public administration entity’ means an entity in a Member State that complies with the following criteria:
- (a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;
  - (b) it has legal personality;
  - (c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law;

---

<sup>8</sup> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p.1).

<sup>9</sup> Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ L 149, 11.6.2005, p. 22).

<sup>10</sup> Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

- (d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

In accordance with the conditions laid down in Article 2(3), public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.

- (24) 'entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;
- (25) 'essential entity' means any entity of a type referred to as an essential entity in Annex I;
- (26) 'important entity' means any entity of a type referred to as an important entity in Annex II.

## CHAPTER II

### Coordinated cybersecurity regulatory frameworks

#### *Article 5*

#### ***National cybersecurity strategy***

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:
  - (a) a definition of objectives and priorities of the Member States' strategy on cybersecurity;
  - (b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors;
  - (c) an assessment to identify relevant assets and cybersecurity risks in that Member State;
  - (d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;
  - (e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;
  - (f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council<sup>11</sup> [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.

---

<sup>11</sup> [insert the full title and OJ publication reference when known]

2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:
  - (a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;
  - (b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;
  - (c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;
  - (d) a policy related to sustaining the general availability and integrity of the public core of the open internet;
  - (e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;
  - (f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;
  - (g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;
  - (h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.
3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is strictly necessary to preserve national security.
4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.

## *Article 6*

### ***Coordinated vulnerability disclosure and a European vulnerability registry***

1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

#### *Article 7*

##### ***National cybersecurity crisis management frameworks***

1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them.
2. Each Member State shall identify capabilities, assets and procedures that can be deployed in case of a crisis for the purposes of this Directive.
3. Each Member State shall adopt a national cybersecurity incident and crisis response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan shall lay down, in particular, the following:
  - (a) objectives of national preparedness measures and activities;
  - (b) tasks and responsibilities of the national competent authorities;
  - (c) crisis management procedures and information exchange channels;
  - (d) preparedness measures, including exercises and training activities;
  - (e) relevant public and private interested parties and infrastructure involved;
  - (f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.
4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.

#### *Article 8*

##### ***National competent authorities and single points of contact***

1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities.

2. The competent authorities referred to paragraph 1 shall monitor the application of this Directive at national level.
3. Each Member State shall designate one national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.
4. Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.
5. Member States shall ensure that the competent authorities referred to in paragraph 1 and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group referred to in Article 12.
6. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts.

#### *Article 9*

#### ***Computer security incident response teams (CSIRTs)***

1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in Article 10(1), covering at least the sectors, subsectors or entities referred to in Annexes I and II, and be responsible for incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority referred to in Article 8.
2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively their tasks as set out in Article 10(2).
3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.
4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities.
5. CSIRTs shall participate in peer reviews organised in accordance with Article 16.

6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 13.
7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1, the CSIRT coordinator designated in accordance with Article 6(1) and their respective tasks provided in relation to the entities referred to in Annexes I and II.
8. Member States may request the assistance of ENISA in developing national CSIRTs.

#### *Article 10*

##### ***Requirements and tasks of CSIRTs***

1. CSIRTs shall comply with the following requirements:
  - (a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;
  - (b) CSIRTs' premises and the supporting information systems shall be located in secure sites;
  - (c) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers;
  - (d) CSIRTs shall be adequately staffed to ensure availability at all times;
  - (e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;
  - (f) CSIRTs shall have the possibility to participate in international cooperation networks.
2. CSIRTs shall have the following tasks:
  - (a) monitoring cyber threats, vulnerabilities and incidents at national level;
  - (b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents;
  - (c) responding to incidents;
  - (d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
  - (e) providing, upon request of an entity, a proactive scanning of the network and information systems used for the provision of their services;
  - (f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request.
3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive.

4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:
- (a) incident handling procedures;
  - (b) cybersecurity crisis management;
  - (c) coordinated vulnerability disclosure.

*Article 11*  
***Cooperation at national level***

1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.
2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20.
3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant to this Directive.
4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council<sup>12</sup> [the DORA Regulation] within that Member State.
5. Member States shall ensure that their competent authorities regularly provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.

---

<sup>12</sup> [insert the full title and OJ publication reference when known]

## CHAPTER III

### *Cooperation*

#### *Article 12*

#### **Cooperation Group**

1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Directive, a Cooperation Group is established.
2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.
3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.

Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.

The Commission shall provide the secretariat.

4. The Cooperation Group shall have the following tasks:
  - (a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;
  - (b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, building capacity as well as standards and technical specifications;
  - (c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;
  - (d) exchanging advice and cooperating with the Commission on draft Commission implementing or delegated acts adopted pursuant to this Directive;
  - (e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;
  - (f) discussing reports on the peer review referred to in Article 16(7);
  - (g) discussing results from joint-supervisory activities in cross-border cases as referred to in Article 34;
  - (h) providing strategic guidance to the CSIRTs network on specific emerging issues;
  - (i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs;
  - (j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges;
  - (k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA.

5. The Cooperation Group may request from the CSIRT network a technical report on selected topics.
6. By ... [ 24 months after the date of entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.
7. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).
8. The Cooperation Group shall meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to promote strategic cooperation and exchange of information.

*Article 13*  
**CSIRTs network**

1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of the national CSIRTs is established.
2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.
3. The CSIRTs network shall have the following tasks:
  - (a) exchanging information on CSIRTs' capabilities;
  - (b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;
  - (c) at the request of a representative of the CSIRT network potentially affected by an incident, exchanging and discussing information in relation to that incident and associated cyber threats, risks and vulnerabilities;
  - (d) at the request of a representative of the CSIRT network, discussing and, where possible, implementing a coordinated response to an incident that has been identified within the jurisdiction of that Member State;
  - (e) providing Member States with support in addressing cross-border incidents pursuant to this Directive;
  - (f) cooperating and providing assistance to designated CSIRTs referred to in Article 6 with regard to the management of multiparty coordinated disclosure of vulnerabilities affecting multiple manufacturers or providers of ICT products, ICT services and ICT processes established in different Member States;
  - (g) discussing and identifying further forms of operational cooperation, including in relation to:
    - (i) categories of cyber threats and incidents;
    - (ii) early warnings;
    - (iii) mutual assistance;

- (iv) principles and modalities for coordination in response to cross-border risks and incidents;
  - (v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3);
  - (h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), where necessary, requesting guidance in that regard;
  - (i) taking stock from cybersecurity exercises, including from those organised by ENISA;
  - (j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;
  - (k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;
  - (l) discussing the peer-review reports referred to in Article 16(7);
  - (m) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.
4. For the purpose of the review referred to in Article 35 and by [24 months after the date of entry into force of this Directive], and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.
5. The CSIRTs network shall adopt its own rules of procedure.

#### *Article 14*

##### ***The European cyber crises liaison organisation network (EU - CyCLONe)***

1. In order to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.
2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information.
3. EU-CyCLONe shall have the following tasks:
  - (a) increasing the level of preparedness of the management of large scale incidents and crises;
  - (b) developing a shared situational awareness of relevant cybersecurity events;
  - (c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis;

- (d) discussing national cybersecurity incident and response plans referred to in Article 7(2).
- 4. EU-CyCLONe shall adopt its rules of procedure.
- 5. EU-CyCLONe shall regularly report to the Cooperation Group on cyber threats, incidents and trends, focusing in particular on their impact on essential and important entities.
- 6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.

#### *Article 15*

##### ***Report on the state of cybersecurity in the Union***

- 1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following:
  - (a) the development of cybersecurity capabilities across the Union;
  - (b) the technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16;
  - (c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities.
- 2. The report shall include particular policy recommendations for increasing the level of cybersecurity across the Union and a summary of the findings for the particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

#### *Article 16*

##### **Peer-reviews**

- 1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by 18 months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed and shall cover at least the following:
  - (i) the effectiveness of the implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;
  - (ii) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the national competent authorities;
  - (iii) the operational capabilities and effectiveness of CSIRTs;
  - (iv) the effectiveness of mutual assistance referred to in Article 34;
  - (v) the effectiveness of the information-sharing framework, referred to in Article 26 of this Directive.

2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.
3. The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors, including targeted issues specific to one or several Member States or one or several sectors.
4. Peer reviews shall entail actual or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects. Any information obtained through the peer review process shall be used solely for that purpose. The experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that review to any third parties.
5. Once reviewed in a Member State, the same aspects shall not be subject to further peer review within that Member State during the two years following the conclusion of a peer review, unless otherwise decided by the Commission, upon consultation with ENISA and the Cooperation Group.
6. Member State shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA without undue delay.
7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. The reports shall be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group.

## **CHAPTER IV**

### ***Cybersecurity risk management and reporting obligations***

#### **SECTION I**

#### ***Cybersecurity risk management and reporting***

##### ***Article 17***

##### ***Governance***

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to

comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.

2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.

## *Article 18*

### ***Cybersecurity risk management measures***

1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network, **services** and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.
2. The measures referred to in paragraph 1 shall include at least the following:
  - (a) **Cyber threat** risk analysis and information system security policies **including for the supply chain**;
  - (b) incident handling (prevention, detection, and response to incidents);
  - (c) **the effectiveness of** business continuity and crisis management, **including for the supply chain**;
  - (d) supply chain, **including entities which provide business services, network and information system services** ~~security including~~ security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;
  - (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - (f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
  - (g) the use of cryptography and encryption.
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.
4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring the service concerned into compliance.
5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

6. The Commission is empowered to adopt ~~delegated~~ **implementing** acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities. **In this case, the technical and organizational requirements shall be at least equivalent than those indicated in the directive.**

#### *Article 19*

##### ***EU coordinated risk assessments of critical supply chains***

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.

**(New) These assessments referred to in paragraphe 1 should be duly taken into account by important and essential entities to comply with requirements identify in Article 18 paragraphe 2 (d).**

2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

#### *Article 20*

##### ***Reporting obligations***

1. Member States shall ensure that essential and important entities 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, **including when those entities are supervised by sector-specific Union legal act.** Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.
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.

Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.

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.~~
4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:
- (a) ~~without undue delay and~~ in any event within ~~24~~ **72** 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;
  - (b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;
  - (c) a final report not later than one month after the submission of the report under point (a), including at least the following:
    - (i) a detailed description of the incident, its severity and impact;
    - (ii) the type of threat or root cause that likely triggered the incident;
    - (iii) applied and ongoing mitigation measures.

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).

5. The competent national authorities or the CSIRT shall provide, ~~within 24 hours~~ **without undue delay** 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. 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. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.
6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States ~~and ENISA~~ of the incident. **When appropriate, Member States may inform ENISA of the incident.** In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.
7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.
8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.
9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near

misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].
- ~~11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).~~

## *Article 21*

### *Use of European cybersecurity certification schemes*

1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities ~~to certify certain ICT products, ICT services and ICT to resort to :~~

**-trust services or notified electronic identification schemes under Regulation 910/2014,**

**-Particular ICT products services and processes certified** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881, **or national certification schemes in the absence of a relevant EU scheme.** The ICT products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

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

2. The Commission ~~shall~~ **may** be empowered to adopt ~~delegated~~ **implementing** acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. ~~The delegated acts shall be adopted in accordance with Article 36. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).~~
3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.

## *Article 22*

### *Standardisation*

1. 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.

2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

### *Article 23*

#### ***Databases of domain names and registration data***

1. For the purpose of contributing to the security, stability and resilience of the DNS, 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 in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.
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.
3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.
4. 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.
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. 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.

## Section II

### **Jurisdiction and Registration**

#### *Article 24*

##### ***Jurisdiction and territoriality***

1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union.
3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive.
4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself.

#### *Article 25*

##### ***Registry for essential and important entities***

1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:
  - (a) the name of the entity;
  - (b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);
  - (c) up-to-date contact details, including email addresses and telephone numbers of the entities.
2. The entities referred to in paragraph 1 shall notify ENISA about any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.

3. Upon receipt of the information under paragraph 1, ENISA shall forward it to the single points of contact depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative. Where an entity referred to in paragraph 1 has besides its main establishment in the Union further establishments in other Member States, ENISA shall also inform the single points of contact of those Member States.
4. Where an entity fails to register its activity or to provide the relevant information within the deadline set out in paragraph 1, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.

## **CHAPTER V**

### ***Information sharing***

#### *Article 26*

#### ***Cybersecurity information-sharing arrangements***

1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:
  - (a) aims at preventing, detecting, responding to or mitigating incidents;
  - (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats' ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.
2. Member States shall ensure that the exchange of information takes place within trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared and in compliance with the rules of Union law referred to in paragraph 1.
3. Member States shall set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).
4. Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.

#### *Article 27*

##### ***Voluntary notification of relevant information***

Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.

### **CHAPTER VI**

#### *Supervision and enforcement*

#### *Article 28*

##### ***General aspects concerning supervision and enforcement***

1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20.
2. Competent authorities shall work in ~~close~~ cooperation with data protection authorities and **other competent authorities designated under sector-specific Union legal act when addressing cybersecurity incidents.**  
~~when addressing incidents resulting in personal data breaches.~~  
**(New) Competent authorities may rely on sectorial or territorial CSIRT.**

#### *Article 29*

##### **Supervision and enforcement for essential entities**

1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:
  - (a) on-site inspections and off-site supervision, including random checks;
  - (b) regular audits;
  - (c) targeted security audits based on risk assessments or risk-related available information;
  - (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;
  - (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);
  - (f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;
  - (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.
3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.
4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:
  - (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;
  - (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;
  - (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;
  - (d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;
  - (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;
  - (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;
  - (g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;
  - ~~(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;~~
  - (i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;
  - (j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or

instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:
- (a) suspend or request a certification or **demand from an** authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;
  - (b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.

These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.
7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:
- (a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.
  - (b) the duration of the infringement, including the element of repeated infringements;
  - (c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;
  - (d) the intentional or negligent character of the infringement;
  - (e) measures taken by the entity to prevent or mitigate the damage and/or losses;
  - (f) adherence to approved codes of conduct or approved certification mechanisms;
  - (g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.

8. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.
9. 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 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.

### *Article 30*

#### **Supervision and enforcement for important entities**

1. When provided with ~~evidence~~ **an incident notification, or substantiation** ~~or indication~~ that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures.
2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to:
  - (a) on-site inspections and off-site *ex post* supervision;
  - (b) targeted security audits based on risk assessments or risk-related available information;
  - (c) security scans based on objective, **non discriminatory**, fair and transparent risk assessment criteria;
  - (d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);
  - (e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.
3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.
4. Member States shall ensure that the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to:
  - (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;
  - (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;
  - (c) order those entities to cease conduct that is in non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;

- (d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;
- (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;
- (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;
- (g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;
- (h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;
- (i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.

**(New) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligation provided for by article 18 and 20.**

5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for the important entities listed in Annex II.

### *Article 31*

#### ***General conditions for imposing administrative fines on essential and important entities***

1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).
3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7).
4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.
5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.
6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what extent administrative

finances may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.

#### *Article 32*

##### ***Infringements entailing a personal data breach***

- ~~1. Where the competent authorities have indications noted that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within a reasonable period of time.~~
- ~~2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58(i) of that Regulation and impose an administrative fine, the competent authorities shall not impose an administrative fine for the same infringement under Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive.~~
- ~~3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority may inform the supervisory authority established in the same Member State.~~

#### *Article 33*

##### **Penalties**

1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.
2. Member States shall, by [two] years following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.

#### *Article 34*

##### **Mutual assistance**

1. Where an essential or important entity is providing services in more than one Member State, or has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or other establishment or of the representative, and the competent authorities of those other Member States shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that:
  - (a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent

authorities in the other Member States concerned on the supervisory and enforcement measures taken and their follow-up, in accordance with Articles 29 and 30;

- (b) a competent authority may request another competent authority to take the supervisory or enforcement measures referred to in Articles 29 and 30;
- (c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance so that the supervision or enforcement actions referred to in Articles 29 and 30 can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed may not refuse that request unless, after an exchange with the other authorities concerned, ENISA and the Commission, it is established that either the authority is not competent to provide the requested assistance or the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out in accordance with Article 29 or Article 30.

2. Where appropriate and with common agreement, competent authorities from different Member States may carry out the joint supervisory actions referred to in Articles 29 and 30.

## **CHAPTER VII**

### *Transitional and final provisions*

#### *Article 35*

##### ***Review***

The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The first report shall be submitted by... [54 months after the date of entry into force of this Directive].

#### *Article 36*

##### ***Exercise of the delegation***

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Articles 18(6) and 21(2) shall be conferred on the Commission for a period of five years from [...]
3. The delegation of power referred to in Articles 18(6) and 21(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the

publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Articles 18(6) and 21(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

#### *Article 37*

##### ***Committee procedure***

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.

#### *Article 38*

##### ***Transposition***

1. Member States shall adopt and publish, by ... [18 months after the date of entry into force of this Directive], the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from ... [one day after the date referred to in the first subparagraph].
2. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

#### *Article 39*

##### ***Amendment of Regulation (EU) No 910/2014***

Article 19 of Regulation (EU) No 910/2014 is deleted.

*Article 40*

***Amendment of Directive (EU) 2018/1972***

Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.

*Article 41*

***Repeal***

Directive (EU) 2016/1148 is repealed with effect from.. [ date of transposition deadline of the Directive].

References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.

*Article 42*

***Entry into force***

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

*Article 43*

***Addressees***

This Directive is addressed to the Member States.

Done at Brussels,

*For the European Parliament*  
*The President*

*For the Council*  
*The President*

**ESSENTIAL ENTITIES:****SECTORS, SUBSECTORS AND TYPES OF ENTITIES**

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of ‘supply’ referred to in point (12) of Article 2 of that Directive <sup>(13)</sup>
		— Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944
		— Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944
		— Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944
		— Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943 <sup>(14)</sup>
		— Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944
	(b) District heating and cooling	— District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 <sup>(15)</sup> on the promotion of the use of energy from renewable sources

<sup>13</sup> Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125).

<sup>14</sup> Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

<sup>15</sup> Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC <sup>(16)</sup>
	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC <sup>(17)</sup>
		— Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators referred to in point (10) of Article 2 of Directive 2009/73/EC
		— LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 <sup>(18)</sup>
		— Airport managing bodies referred to

<sup>16</sup> Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).

<sup>17</sup> Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

<sup>18</sup> Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72).

		in point (2) of Article 2 of Directive 2009/12/EC <sup>(19)</sup> , airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 <sup>(20)</sup> , and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004 <sup>(21)</sup>
	(b) Rail	— Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU <sup>(22)</sup>
		— Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 <sup>(23)</sup> , not including the individual vessels operated by those companies
		— Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC <sup>(24)</sup> , including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating

<sup>19</sup> Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11).

<sup>20</sup> Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1).

<sup>21</sup> Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p.1).

<sup>22</sup> Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).

<sup>23</sup> Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6).

<sup>24</sup> Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

		works and equipment contained within ports
		— Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC <sup>(25)</sup>
	(d) Road	— Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 <sup>(26)</sup> responsible for traffic management control
		— Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU <sup>(27)</sup>
3. Banking		Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 <sup>(28)</sup>
4. Financial market infrastructures		— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU <sup>(29)</sup>
		— Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012 <sup>(30)</sup>
5. Health		— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU <sup>(31)</sup>

<sup>25</sup> Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10)

<sup>26</sup> Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

<sup>27</sup> Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

<sup>28</sup> Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

<sup>29</sup> Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

<sup>30</sup> Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

<sup>31</sup> Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

		<p>— EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health<sup>32</sup></p>
		<p>— Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC<sup>(33)</sup></p> <p>— Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2</p> <p>— Entities manufacturing medical devices considered as critical during a public health emergency ('the public health emergency critical devices list') referred to in Article 20 of Regulation XXXX<sup>34</sup></p>
6. Drinking water		Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC <sup>(35)</sup> but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential or important services
7. Waste water		Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC <sup>(36)</sup>
8. Digital infrastructure		<p>— Internet Exchange Point providers</p> <p>— DNS service providers</p>

<sup>32</sup> [Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted]

<sup>33</sup> Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67).

<sup>34</sup> [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]

<sup>35</sup> Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

<sup>36</sup> Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p.40).

		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		— Content delivery network providers
		— Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014 <sup>(37)</sup>
		— Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972 <sup>(38)</sup> 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
9. Public administration		— Public administration entities of central governments
		<del>— Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003<sup>(39)</sup></del>
		<del>— Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003</del>
10. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972

<sup>37</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73).

<sup>38</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).

<sup>39</sup> Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).

## ANNEX II

### **IMPORTANT ENTITIES:**

#### **SECTORS, SUBSECTORS AND TYPES OF ENTITIES**

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC <sup>(40)</sup> and providers of courier services
2. Waste management		Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC <sup>(41)</sup> but excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture, production and distribution of substances and articles referred to in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 <sup>(42)</sup>
4. Food production, processing and distribution		Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 <sup>(43)</sup>
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745 <sup>(44)</sup> , and entities manufacturing in vitro diagnostic medical devices referred to

<sup>40</sup> Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14).

<sup>41</sup> Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)

<sup>42</sup> Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

<sup>43</sup> Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).

<sup>44</sup> Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1)

		in Article 2 point 2 of Regulation (EU) 2017/746 <sup>(45)</sup> with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		— Providers of online marketplaces
		— Providers of online search engines
		— Providers of social networking services platform

<sup>45</sup> Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p.176)

*ANNEX III*

***CORRELATION TABLE***

<b>Directive (EU) 2016/1148</b>	<b>This Directive</b>
Article 1 (1)	Article 1 (1)
Article 1 (2)	Article 1 (2)
Article 1 (3)	-
Article 1 (4)	Article 2 (4)
Article 1 (5)	Article 2 (5)
Article 1 (6)	Article 2 (3)
Article 1 (7)	Article 2 (6)
Article 2	-
Article 3	Article 3
Article 4	Article 4
Article 5	-
Article 6	-
Article 7 (1)	Article 5 (1)
Article 7 (2)	Article 5 (4)
Article 7 (3)	Article 5 (3)
Article 8 (1)–(5)	Article 8 (1)–(5)
Article 8 (6)	Article 11 (4)
Article 8 (7)	Article 8 (6)
Article 9 (1)-(3)	Article 9 (1)-(3)
Article 9 (4)	Article 9 (7)
Article 9 (5)	Article 9 (8)
Article 10 (1)-(3)	Article 11 (1)-(3)
Article 11 (1)	Article 12 (1) –(2)

Article 11 (2)	Article 12 (3)
Article 11 (3)	Article 12(4) and (6)
Article 11 (4)	-
Article 11 (5)	Article 12 (7)
Article 12 (1)-(5)	Article 13 (1)-(5)
Article 13	-
Article 14 (1)	Article 18 (1)
Article 14 (2)	Article 18 (2)-(4)
Article 14 (3)	Article 20 (1)
Article 14 (4)	Article 20 (3)
Article 14 (5)	Article 20 (5), (6), (8)
Article 14 (6)	Article 20 (7)
Article 14 (7)	-
Article 15 (1)	Article 29 (2)
Article 15 (2)(a)	Article 29 (2) (e)
Article 15 (2)(b)	Article 29 (2) (g)
Article 15 (2) second indent	Article 29 (3)
Article 15 (3)	Article 29 (4) (b)
Article 15 (4)	Article 28 (2)
Article 16 (1)	Article 18 (1), (2)
Article 16 (2)	Article 18 (2)-(4)
Article 16 (3)	Article 20 (1)
Article 16 (4)	Article 20 (3)
Article 16 (5)	-
Article 16 (6)	Article 20 (6)
Article 16 (7)	Article 20 (7)
Article 16 (8), (9)	Article 20 (11)

Article 16 (10)	-
Article 16 (11)	Article 2 (1)
Article 17 (1)	-
Article 17 (2)(a)	Article 29 (2) (e)
Article 17 (2)(b)	Article 29 (4) (b)
Article 17 (3)	Article 34 (1) (a), (b)
Article 18 (1)	Article 24 (1)-(2)
Article 18 (2)	Article 24 (3)
Article 18 (3)	Article 24 (4)
Article 19	Article 22
Article 20	Article 27
Article 21	Article 33
Article 22 (1)-(2)	Article 37 (1)-(2)
Article 23	Article 35
Article 24	-
Article 25	Article 38
Article 26	Article 42
Article 27	Article 43
Annex I(1)	Article 10 (1)
Annex I (2) (a) (i)-(iv)	Article 10 (2) (a)-(d)
Annex I (2) (a) (v)	Article 10 (2) (f)
Annex I (2) (b)	Article 10 (3)
Annex I (2) (c) (i)-(ii)	Article 10 (4) (a)
Annex II	Annex I
Annex III 1, 2	Annex II, 6.
Annex III, 3	Annex I, 8.

## GERMANY

Horizontal Working Party on Cyber Issues – Drafting COM(2020) 823 final (NIS2)

### Change requests and drafting proposals for Article 2 NIS2 by DE

24 June 2021

Preliminary note: The PT-Presidency asked Member States to submit their change requests and drafting proposals regarding Article 2 NIS2 as well as changes to the Annexes I and II, Articles 17-22 (requirements) and Articles 29-30 (supervision / sanctions) until 24 June 2021. This exercise is to provide the SI-Presidency with the necessary input by Member States in order for it to draft a compromise proposal for this central provision of NIS2. This document contains the current change requests and drafting proposals by Germany until that time. Please note that the proposed changes have implications throughout the entire proposal. Some of the Non-Papers co-signed by DE and referenced below contain further drafting proposals and we have not included them in this table. There may be other changes required, which we will submit at a later stage after further deliberations.

No.	COM(2020) 823 final	Drafting proposal	Justification
1.	<p><i>Article 2</i></p> <p><b>Scope</b></p> <p>1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises</p>	<p><i>Article 2</i></p> <p><b>Scope</b></p> <p>1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises</p>	<ul style="list-style-type: none"> <li>Regarding para. 1 sentence 1 – Together with NL and others, we propose to consolidate both categories of entities into the lower category (important entities) and allow Member States to select those entities that should belong to the higher category (essential entities). This may entail the consolidation of Annexes I and II into one. However, text proposals were not yet included and will be presented in a subsequent iteration of the Non-Paper. For further details</li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
	within the meaning of Commission Recommendation 2003/361/EC.	within the meaning of Commission Recommendation 2003/361/EC. <b>Article 3 paragraph 4 of Commission Recommendation 2003/361/EC shall not apply.</b>	<p>on the concept, please refer to the Non-Paper <i>On the scope of NIS</i> co-signed by DE and submitted to the Presidency on 24 June.</p> <ul style="list-style-type: none"> <li>Regarding para. 1 sentence 2 – The referenced Commission Recommendation states that enterprises that are publicly owned by 25 % or more cannot be considered SME. Therefore, publicly owned or municipal companies cannot be considered SME even if they only have one employee and would therefore be in the scope of NIS2.</li> </ul>
2.		<p><b>1a. This Directive also applies to public administration entities indentified by the Member States in accordance with art. 2a, notwithstanding para 1b.</b></p> <p><del><b>1b. This Directive does not apply to public administration entities that carry out activities in the areas of public security, defence or national security.</b></del></p>	<ul style="list-style-type: none"> <li>Regarding para. 1a – Together with PL and others, we propose that Member States retain full decision-making autonomy regarding the question of whether to identify public administration entities and if Member States decided to do so which entities are to be identified. For further details, please refer to the Non-Paper <i>On the inclusion of public administration in the NIS2 directive framework</i> co-signed by DE and submitted to the Presidency on 24 June.</li> <li>Regarding para. 1b – This specific exclusion included in the aforementioned non-paper is not necessary if the issue is addressed by way of amending the general exclusion clause in Article 2 para. 3, as proposed in table row 4. below.</li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
3.	<p>2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:</p> <p>(a) the services are provided by one of the following entities:</p> <p>(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;</p> <p>(ii) trust service providers referred to point 8 of Annex I;</p> <p>(iii) top-level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;</p> <p>(b) the entity is a public administration entity as defined in point 23 of Article 4;</p> <p>(c) the entity is the sole provider of a service in a Member State;</p> <p>(d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;</p> <p>(e) a potential disruption of the</p>	<p>2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:</p> <p>(a) the services are provided by one of the following entities:</p> <p>(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;</p> <p>(ii) trust service providers referred to point 8 of Annex I;</p> <p>(iii) top-level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;</p> <p><del>(b) the entity is a public administration entity as defined in point 23 of Article 4;</del></p> <p>(eb) the entity is the sole provider of a service in a Member State;</p> <p><del>(dc)</del> a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;</p> <p>(ed) a potential disruption of the</p>	<ul style="list-style-type: none"> <li>Regarding para. 2 sentence 2 – We propose to delete the obligation by Member States to compile and submit a list of entities. There is no apparent necessity or use case for such a list that would justify the associated security risk.</li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
	<p>service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;</p> <p>(f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;</p> <p>(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.</p> <p>Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.</p>	<p>service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;</p> <p>(fe) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;</p> <p>(gf) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.</p> <p><del>Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.</del></p>	
4.	3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public	3. This Directive <b>does not</b> (a) <del>is without prejudice to the</del>	<ul style="list-style-type: none"> <li>Together with SE and others, we think that the current exclusion clause (i) does not clearly reflect the need to exclude relevant entities</li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
	<p>security, defence and national security in compliance with Union law.</p>	<p><del>competences affect the sole responsibility of Member States to safeguard concerning the maintenance of public security, defence and national security or their power to protect other essential State functions . In particular, this Directive does not</del></p> <p>(i) apply to entities with importance to Member States' defence or national security,</p> <p>(ii) oblige Member States or entities to supply information where such a supply of information would be contrary to national security or defence interests,</p> <p>(iii) apply to those activities of entities, which fall outside the scope of <del>in compliance with</del> Union law and in any event all activities concerning national security and defence, regardless of who is carrying out those activities whether it is a public entity or a private entity acting at the request of a public</p>	<p>entirely, (ii) does not contain a clear statement that Member States should not be under any obligation to supply relevant information and (iii) does not clearly exclude relevant activities by entities that are otherwise in scope of NIS2.</p> <ul style="list-style-type: none"> <li>• We propose to model the exclusion clause after the Council draft of Article 2 ePrivacy regulation of 10 February 2021 and thereby address the issues described above. For further details on the proposal for a revised exclusion clause, please refer to the Non-Paper <i>NIS2 Exclusion Clause</i> co-signed by DE and submitted to the Presidency on 24 June.</li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
		<p>entity.</p> <p>(b) apply in the area of public security and the judiciary. In particular, this Directive does not</p> <p>(i) apply to entities with importance to Member States' judiciary and public security, including public administration entities to any extent concerned with law enforcement,</p> <p>(ii) oblige Member States or entities to supply information where such a supply of information would be contrary to public security,</p> <p>(iii) apply to those activities of entities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.</p>	
5.		3a. This Directive is without prejudice to Union law on the protection of	<ul style="list-style-type: none"> <li>This drafting proposal was already included in the <i>Presidency Compromise Proposal on</i></li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
		<b>personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.</b>	<i>NIS2 Interaction with Sectoral Legislation</i> dated 9 June 2021 (doc. ST 09583/21) and is included here only for the sake of completeness.
6.	4. This Directive applies without prejudice to Council Directive 2008/114/EC and Directives 2011/93/EU and 2013/40/EU of the European Parliament and of the Council.	4. This Directive applies without prejudice to Council Directive 2008/114/EC and Directives 2011/93/EU and 2013/40/EU of the European Parliament and of the Council.	
7.	5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.	5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.	
8.	6. Where provisions of sector-specific acts of Union law require essential or important entities either to adopt	6. Where provisions of sector-specific <b>Union legal</b> acts of Union law require essential or important entities either to	<ul style="list-style-type: none"> <li>This drafting proposal was already included in the <i>Presidency Compromise Proposal on NIS2 Interaction with Sectoral Legislation</i></li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
	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.	adopt cybersecurity risk management measures or to notify <b>significant</b> incidents or <del>significant</del> 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 <b>to those entities</b> .	dated 9 June 2021 (doc. ST 09583/21) and is included here only for the sake of completeness.
9.		<p><b>7. In order to safeguard a coherent minimum standard of cybersecurity across all sectors, sector-specific Union legal acts referred to in paragraph 6 should include</b></p> <p><b>(a) cybersecurity risk management measures, that are at a minimum equivalent to those laid down in article 18 paragraphs 1 and 2 of this Directive; and</b></p> <p><b>(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:</b></p> <p><b>(i) automatic and direct access to the incident notifications by the national competent authority under this</b></p>	<ul style="list-style-type: none"> <li>Regarding para. 7 (a) through (b) – This drafting proposal was already – in principle – included in the <i>Presidency Compromise Proposal on NIS2 Interaction with Sectoral Legislation</i> dated 21 June 2021 (doc. ST 09583/1/21 REV 1) and is included here only for the sake of completeness.</li> <li>Regarding para. 7 (c) – In order to safeguard a coherent minimum standard of cybersecurity across all sectors, the involvement of the NIS competent authorities is necessary in the supervision and enforcement of cybersecurity risk management measures and of requirements to notify incidents or significant cyber threats.</li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
		<p>Directive through a common reporting mechanism; or</p> <p>(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 Union legal act.</p> <p>(c) provisions for the consultation of the national competent authority under this Directive regarding supervision and enforcement of cybersecurity risk management measures and of requirements to notify incidents or significant cyber threats.</p>	
10.		<p><i>Article 2a</i></p> <p><i>Identification of Public Administration Entities</i></p> <ol style="list-style-type: none"> <li>1. By [date] Member States may identify public administration entities established on their territory.</li> <li>2. The criteria for the progressive identification of public administration entities shall be as</li> </ol>	<ul style="list-style-type: none"> <li>• For further details on our proposal with PL and others, please refer to the Non-Paper <i>On the inclusion of public administration in the NIS2 directive framework</i> co-signed by DE and submitted to the Presidency on 24 June.</li> </ul>

No.	COM(2020) 823 final	Drafting proposal	Justification
		<p>follows:</p> <ul style="list-style-type: none"> <li>(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;</li> <li>(b) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law;</li> <li>(c) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.</li> </ul> <p>3. The public administration entities identified in line with this Article shall be reviewed and where appropriate updated by Member States when necessary.</p> <p>4. Member States shall inform the</p>	

No.	COM(2020) 823 final	Drafting proposal	Justification
		<b>Commission about the result of the process of identification of public administration entities in accordance with this Article.</b>	

\* \* \*

## Article 2

### Scope

1. This Directive applies to private entities identified by the Member States as essential entities in the sectors and subsectors referred to in Annex I and to important entities who carry out their main activity in the sectors and subsectors of Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.<sup>46</sup>
2. The criteria for the identification of the essential entities shall be as follows:
  - (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
  - (b) the provision of that service depends on network and information systems; and
  - (c) an incident would have significant disruptive effects on the provision of that service.
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;
  - (c) the entity is the sole provider of a service in a Member State;
  - (d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;
  - (e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;
  - (f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;

---

<sup>46</sup> Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

- (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council<sup>47</sup> [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.

Member States shall establish a list of entities identified pursuant to points (b) to (e) and submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.

3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.
4. This Directive applies without prejudice to Council Directive 2008/114/EC<sup>48</sup> and Directives 2011/93/EU<sup>49</sup> and 2013/40/EU<sup>50</sup> of the European Parliament and of the Council.
5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.
6. 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.

## CHAPTER IV

### *Cybersecurity risk management and reporting obligations*

#### SECTION I

##### *Cybersecurity risk management and reporting*

---

<sup>47</sup> [insert the full title and OJ publication reference when known]

<sup>48</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

<sup>49</sup> Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

<sup>50</sup> Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

## *Article 17*

### ***Governance***

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.
2. Member States shall ensure that members of the management body follow specific trainings to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.

## *Article 18*

### ***Cybersecurity risk management measures***

1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network 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.
2. The measures referred to in paragraph 1 shall include at least the following:
  - (a) risk analysis and information system security policies;
  - (b) incident handling (prevention, detection, and response to incidents);
  - (c) business continuity and crisis management;
  - (d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;
  - (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - (f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
  - (g) the use of cryptography and encryption.
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures and vulnerability management practices.
4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring the service concerned into compliance.

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

6.

## *Article 19*

### ***EU coordinated risk assessments of critical supply chains***

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.
2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

## *Article 20*

### ***Reporting obligations***

1. Member States shall ensure that essential and important entities 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 recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.
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.

Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.
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.
4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:

- (a) 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;
- (b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;
- (c) a final report not later than one month after the submission of the report under point (a), including at least the following:
  - (i) a detailed description of the incident, its severity and impact;
  - (ii) the type of threat or root cause that likely triggered the incident;
  - (iii) applied and ongoing mitigation measures.

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).

5. The competent national authorities or the CSIRT shall provide without undue delay 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. 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. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.
6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.
7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.
8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.
9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.
10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing act  
s to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

## *Article 22*

### ***Standardisation***

1. 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.
2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

## **CHAPTER VI**

### *Supervision and enforcement*

## *Article 28*

### ***General aspects concerning supervision and enforcement***

1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20.
2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.

## *Article 29*

### **Supervision and enforcement for essential entities**

1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.
2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:

- (a) on-site inspections and off-site supervision, including random checks;
  - (b) regular audits;
  - (c) targeted security audits based on risk assessments or risk-related available information;
  - (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;
  - (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);
  - (f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;
  - (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.
3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.
4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:
- (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;
  - (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;
  - (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;
  - (d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;
  - (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;
  - (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;
  - (g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;
  - (i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;
  - (j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:
- (a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;
  - (b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.

These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.
7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:
- (a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.
  - (b) the duration of the infringement, including the element of repeated infringements;
  - (c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;
  - (d) the intentional or negligent character of the infringement;
  - (e) measures taken by the entity to prevent or mitigate the damage and/or losses;
  - (f) adherence to approved codes of conduct or approved certification mechanisms;
  - (g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.

8. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.
9. 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 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.

### *Article 30*

#### **Supervision and enforcement for important entities**

1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures.
2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to:
  - (a) on-site inspections and off-site *ex post* supervision;
  - (b) targeted security audits based on risk assessments or risk-related available information;
  - (c) security scans based on objective, fair and transparent risk assessment criteria;
  - (d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);
  - (e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.
3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.
4. Member States shall ensure that the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to:
  - (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;
  - (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;
  - (c) order those entities to cease conduct that is in non-compliance with the obligations laid down in this Directive and desist from repeating that conduct;

- (d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;
  - (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;
  - (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;
  - (g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;
  - (h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;
  - (i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.
5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for the important entities listed in Annex II.

### *Article 31*

#### ***General conditions for imposing administrative fines on essential and important entities***

1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).
3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7).
4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.
5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.
6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.

## *Article 32*

### ***Infringements entailing a personal data breach***

1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within a reasonable period of time.
2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58(i) of that Regulation and impose an administrative fine, the competent authorities shall not impose an administrative fine for the same infringement under Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive.
3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority may inform the supervisory authority established in the same Member State.

## *Article 33*

### **Penalties**

1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.
2. Member States shall, by [two] years following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.

# ANNEX I

## ESSENTIAL ENTITIES:

### SECTORS, SUBSECTORS AND TYPES OF ENTITIES

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of ‘supply’ referred to in point (12) of Article 2 of that Directive <sup>(51)</sup>
		— Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944
		— Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944
		— Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944
		(1) Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943 <sup>(52)</sup>
		— Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944
	(b) District heating and cooling	— District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 <sup>(53)</sup> on the promotion of the use of energy from renewable sources

51 Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125).

52 Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

53 Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		10. Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC <sup>(54)</sup>
	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC <sup>(55)</sup>
		— Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators referred to in point (10) of Article 2 of Directive 2009/73/EC
		— LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers conducting commercial air traffic referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 <sup>(56)</sup>
		— Airport managing bodies referred to

54 Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).

55 Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

56 Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72).

		<p>in point (2) of Article 2 of Directive 2009/12/EC<sup>(57)</sup>, airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013<sup>(58)</sup>, and entities operating ancillary installations contained within airports</p>
		<p>— Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004<sup>(59)</sup></p>
	(b) Rail	<p>— Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU<sup>(60)</sup></p> <p>— Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU</p>
	(c) Water	<p>— Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004<sup>(61)</sup>, not including the individual vessels operated by those companies</p> <p>— Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC<sup>(62)</sup>, including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating</p>

57 Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11).

58 Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1).

59 Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p.1).

60 Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).

61 Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6).

62 Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

		works and equipment contained within ports
		— Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC <sup>(63)</sup>
	(d) Road	— Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 <sup>(64)</sup> responsible for traffic management control
		— Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU <sup>(65)</sup>
3. Banking		Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 <sup>(66)</sup>
4. Financial market infrastructures		— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU <sup>(67)</sup>
		— Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012 <sup>(68)</sup>
5. Health		(2) Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU <sup>(69)</sup>

63 Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10)

64 Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

65 Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

66 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

67 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

68 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

69 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

		<p>(3) EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health<sup>70</sup></p> <p>(4) Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC <sup>(71)</sup></p> <p>(5) Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2</p> <p>(6) Entities manufacturing medical devices considered as critical during a public health emergency ('the public health emergency critical devices list') referred to in Article 20 of Regulation XXXX<sup>72</sup></p>
6. Drinking water		Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC <sup>(73)</sup> but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential or important services
7. Waste water		Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC <sup>(74)</sup>

70 [Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted]

71 Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67).

72 [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]

73 Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

74 Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p.40).

8. Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers
		— TLD name registries
		1. Cloud computing service providers
		— Data centre service providers
		(7) Content delivery network providers
		— Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014 <sup>(75)</sup>
		— Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972 <sup>(76)</sup> 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
		(8)
		(9)
		(10)
10. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972

<sup>75</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73).

<sup>76</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).

## ANNEX II

### **IMPORTANT ENTITIES:**

#### **SECTORS, SUBSECTORS AND TYPES OF ENTITIES**

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC <sup>(78)</sup> and providers of courier services
2. Waste management		Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC <sup>(79)</sup> but excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Operators under DIRECTIVE 2012/18/EU
4. Food production, processing and distribution		Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 <sup>(81)</sup>
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745 <sup>(82)</sup> , and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 <sup>(83)</sup> with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.

78 Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14).

79 Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)

81 Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).

82 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1)

83 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p.176)

	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		— Providers of online marketplaces
		— Providers of online search engines
		— Providers of social networking services platform

## IRELAND

### **Comments and Drafting Suggestions from Ireland in response to Request for comments and initial drafting proposals on Article 2 and Annexes, and Articles 17-22, 28-33**

Ireland welcomes the opportunity to provide drafting suggestions in regard to the scope of the proposed Directive, on the substantive obligatory provisions and on the supervision and enforcement aspects of NIS2.

On scope, Ireland proposes that public administration entities remain within scope unless Member States already have equivalent legal obligations in national law on such entities. Ireland also proposes a robust exclusion clause to exempt national security, defence, public security, law enforcement and judicial authorities aspects from the scope. A self registration facility is also proposed in Article 2 so that Member States can engage with identified essential and important entities.

The size cap should be set at higher than medium sized enterprises for an initial period of 2.5 years after transposition so as to enable Member States to implement the Directive on large enterprises and build up capabilities and resources. A lowering of the size cap is provided for in the review clause in Article 35.

A more granular approach is proposed for security requirements in Article 18(2). A similar approach is taken in regards to amendments proposed for reporting in Article 20, with notifications limited to incidents.

Article 19 should be subsumed into Article 12 as it is in essence the business of the cooperation group to undertake coordinated risk assessments.

In Article 21, there is scope for use of certification schemes in connection with supply chain security matters. However there should be no requirements under delegated or implementing acts as there is a separate pathway for mandatory certification schemes under Article 56(3) of the EU Cybersecurity Act.

Ireland also suggests separating supervision from enforcement into separate Articles. This will provide for possibilities for cross border cooperation on supervision while enforcement remains a sole national competence. A prioritisation of the supervision of essential entities is proposed based on the list of entities required in Article 2(2), identified critical entities under CER that are also essential entities and those essential entities in the ENISA registry. On supervision there needs to be liability exemptions for competent authorities.

On enforcement, a proportionate approach needs to be taken with recognition of the Fundamental Rights of individuals. Any process to suspend a service of an essential entity needs to be underpinned by a Court of law.

On the Annexes, managed security service providers should be included under digital infrastructure as a category of essential entity and a new sector for education and research needs to be added to Annex II.

Suggested amendments are set out in the following pages.

### IE Amendments and Comments

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**

### *Article 2*

#### ***Scope***

1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro, small and medium enterprises within the meaning of Commission Recommendation 2003/361/EC.<sup>84</sup>
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;
  - (b) the entity is a public administration entity as defined in point 23 of Article 4 unless such an entity is already subject to security and reporting obligations under national legislation on cybersecurity and such legislation has been assessed by the Member State concerned as at least equivalent in effect to the requirements set out in this Directive;
  - (c) the entity is the sole provider of a service in a Member State;
  - (d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;

---

<sup>84</sup> Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

- (e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;
- (f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;
- (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council<sup>85</sup> [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.

Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit relevant information about the list to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it. Relevant information may include the number of specific entities identified for each category from (b) to (f), the corresponding sectors and types of entities as set out in Annex I and II.

- 2a Member States may, through various designated competent authorities, establish a self registration facility or facilities for all entities who meet the requirements for essential and important entities under paragraphs 1 and 2. In which case Member States can require such entities to provide information similar to that required under Article 25(1) for the purposes of supervision and enforcement.

3. This Directive does not

- (a) affect the sole responsibility of Member States to safeguard national security or their power to protect other essential State functions . In particular, this Directive does not
  - (i) apply to entities with importance to Member States' defence or national security,
  - (ii) oblige Member States or entities to supply information where such a supply of information would be contrary to national security or defence interests,
  - (iii) apply to those activities of entities, which fall outside the scope of Union law and in any event all activities concerning national security and defence, regardless of who is carrying out those activities whether it is a public entity or a private entity acting at the request of a public entity.
- (b) apply in the area of public security and the judiciary. In particular, this Directive does not

---

<sup>85</sup> *[insert the full title and OJ publication reference when known]*

- (i) apply to entities with importance to Member States' judiciary and public security, including public administration entities to any extent concerned with law enforcement,
- (ii) oblige Member States or entities to supply information where such a supply of information would be contrary to public security,
- (iii) apply to those activities of entities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security..

## CHAPTER IV

### *Cybersecurity risk management and reporting obligations*

#### SECTION I

##### *Cybersecurity risk management and reporting*

###### *Article 17*

###### ***Governance***

3. The application of this Article shall be without prejudice to public administration entities that are directed by elected representatives in accordance with the Member State's constitutional legal order.

###### *Article 18*

###### ***Cybersecurity risk management measures***

2. The measures referred to in paragraph 1 shall include at least the following:
  - (a) risk analysis and information system security policies;
  - (b) incident handling (prevention, detection, response to and recovery from incidents);
  - (c) business continuity and crisis management, encompassing as appropriate, documented plans and procedures, defined recovery time objectives and periodic exercising of those plans and procedures;
  - (d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers where a contract exists;

- (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - (f) policies and procedures (testing and auditing) to defined industry standards and best practises on assessing the effectiveness of cybersecurity risk management measures, including, where appropriate, periodic use of security assessments, automated scanning and threat led penetration testing;
  - (g) the use, where appropriate, of cryptography and encryption.
5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, industry standards and best practises, international and European standards, as well as relevant technical specifications.

#### *Article 12*

- 4b. The Cooperation Group, , may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.

2.

## *Article 20*

### ***Reporting obligations***

1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any large scale incident or other such incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.
- 2.
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 losses.
4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:
  - (a) without undue delay and in any event within 72 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 and whether a data breach under Regulation (EU) 2016/679 or Directive 2002/58/EC has occurred;
  - (b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;

- (c) a comprehensive report not later than one month after the submission of the report under point (a), including at least the following:
  - (i) a detailed description of the incident, its severity and impact;
  - (ii) the type of threat or root cause that likely triggered the incident;
  - (iii) applied and ongoing mitigation measures;
  - (iv) the activities taken as regards reporting of malicious actions to law enforcement authorities and reporting of data breaches to supervisory authorities under Regulation (EU) 2016/679 and Directive 2002/58/EC.
- (d) a final report not later than one month after the completion of the recovery and subsequent investigation of the incident, which should be within 12 months after submission of the report under point (a), with this report including the definitively identified root cause, consequential updates to the risk management measures and any other conclusions arising.

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).

5. The competent national authorities or the CSIRT shall endeavour to 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. 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 without any acceptance of liability for consequential actions taken by that entity. The CSIRT shall provide additional technical support if the concerned entity so requests without any acceptance of liability for consequential actions taken by that entity.. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.
6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident and provide relevant threat information. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.
9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraph 1 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report, including on the status of notification reports received under paragraph 4. ENISA shall provide monthly reports on notified incidents in the Union to the Cooperation Group and as appropriate the CSIRTs Network. Such monthly reports shall include commentary on trends and be sufficiently granular to cover all of the sectors, subsectors and types of entity in Annexes I and II.
10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraph 1 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].
11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 4. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3 and the format of summary reports required under paragraph 9. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

## *Article 21*

### ***Use of European cybersecurity certification schemes***

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

- 1a Member States may rely on cybersecurity service providers certified under Regulation (EU) 2019/881 to demonstrate compliance with particular requirements of Article 18, or to enforce supervision activities foreseen in Articles 29 and 30.

2.

3. The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in order to facilitate improved supply chain security of essential and important entities as referenced in Article 18. .

## **CHAPTER VI**

### *Supervision and enforcement*

#### *Article 28*

#### ***General aspects concerning supervision and enforcement***

1. Member States shall ensure that relevant competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20.

#### *Article 29*

#### **Supervision for essential entities**

1. Member States shall ensure that the measures of supervision imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.
2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:
- (a) on-site inspections and off-site supervision, including random checks;
  - (b) regular compliance audits, which may or may not involve penetration testing;
  - (c) targeted security audits based on risk assessments or risk-related available information;

- (d) where appropriate security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;
  - (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);
  - (f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;
  - (g) requests for demonstration of implementation of cybersecurity policies, such as the results of security audits carried out by an independent certified auditor in accordance with industry best practise, training and awareness programmes and defence in depth infrastructure and facilities..
3. Competent authorities shall be exempt from any liability in the course of exercising their supervisory tasks.
4. Competent authorities shall prioritise exercising their supervisory tasks on those essential entities that are:
- in the list established by Member States under Article 2(2);
  - identified as critical entities pursuant to Directive (EU) XXXX/XXXX [CER Directive], and;
  - registered with ENISA pursuant to Article 25.
- Competent authorities shall only exercise their supervisory tasks on other essential entities there they have sufficient resources to do so and where there is information or it is demonstrated that such other essential entities may not be in compliance with the obligations laid down in Articles 18 and 20 of this Directive.
5. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.

#### *Article 29a*

#### **Enforcement for Essential Entities**

1. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:
- (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;
  - (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;
  - (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;

- (d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;
- (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;
- (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;
- (g) designate a monitoring officer, acting as an agent of the competent authority, with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;
- (h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;
- (i) make a public statement which identifies the legal person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;
- (j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

In exercising their enforcement powers under this paragraph, competent authorities may seek Court orders to reinforce their implementation.

2. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (1) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power through their national Courts to order the suspension of all or part of the services or of the public functions of the essential entity.

This sanction shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such a sanction was applied.

3. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.
4. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 1 and 2, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:
  - (a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.
  - (b) the duration of the infringement, including the element of repeated infringements;
  - (c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;
  - (e) measures taken by the entity to prevent or mitigate the damage and/or losses;
  - (f) adherence to approved codes of conduct or approved certification mechanisms;
  - (g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.
5. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.
6. Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities within that same Member State designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Where appropriate competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] may request competent authorities under this Directive to exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

## Article 30

### Supervision for important entities

1. When provided with information or when it is demonstrated that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures.
2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to:
  - (a) on-site inspections and off-site *ex post* supervision;
  - (b) targeted security audits based on risk assessments or risk-related available information;
  - (c) where appropriate, undertake security scans based on objective, fair and transparent risk assessment criteria;
  - (d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);
  - (e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.
3. Competent authorities shall be exempt from any liability in the course of exercising their supervisory tasks.
4. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.

## Article 30a

### Enforcement for important entities

1. Member States shall ensure that the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to:
  - (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;
  - (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;
  - (c) order those entities to cease conduct that is in non-compliance with the obligations laid down in this Directive and desist from repeating that conduct;

- (d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;
  - (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;
  - (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;
  - (g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;
  - (h) make a public statement which identifies the legal person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;
  - (i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.
2. Article 29a (3) to (5) shall also apply to the enforcement measures provided for in this Article for the important entities listed in Annex II.

### *Article 31*

#### ***General conditions for imposing administrative fines on essential and important entities***

- 2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29a(1), Article 29a(2) and points (a) to (h) of Article 30a(1).
- 3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29a(4).
- 4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.
- 5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.
- 6. Without prejudice to the powers of competent authorities pursuant to Articles 29a and 30a, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.

## *Article 32*

### ***Infringements entailing a personal data breach***

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

## **CHAPTER VII**

### *Transitional and final provisions*

## *Article 35*

### ***Review and Extension of Scope***

The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The first report shall be submitted by... [54 months after the date of entry into force of this Directive].

By the date of submission of the first report, and notwithstanding Article 2(1), this Directive shall also apply to entities that qualify as medium enterprises within the meaning of Commission Recommendation 2003/361/EC.

# ANNEX I

## essential entities:

### Sectors, subsectors and types of entities

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of ‘supply’ referred to in point (12) of Article 2 of that Directive <sup>(86)</sup>
		— Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944
		— Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944
		— Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944
		Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943 <sup>(87)</sup>
		— Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of

<sup>86</sup> Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125).

<sup>87</sup> Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

		Directive (EU) 2019/944
	(b) District heating and cooling	— District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 <sup>(88)</sup> on the promotion of the use of energy from renewable sources
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC <sup>(89)</sup>
	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC <sup>(90)</sup>
		— Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators referred to in point (10) of Article 2 of Directive 2009/73/EC

<sup>88</sup> Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

<sup>89</sup> Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).

<sup>90</sup> Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

		— LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 <sup>(91)</sup>
		— Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC <sup>(92)</sup> , airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 <sup>(93)</sup> , and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services referred to in point (1)

<sup>91</sup> Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72).

<sup>92</sup> Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11).

<sup>93</sup> Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1).

		of Article 2 of Regulation (EC) No 549/2004 <sup>(94)</sup>
(b) Rail	—	Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU <sup>(95)</sup>
	—	Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU
(c) Water	—	Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 <sup>(96)</sup> , not including the individual vessels operated by those companies
	—	Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC <sup>(97)</sup> , including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports

<sup>94</sup> Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p.1).

<sup>95</sup> Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).

<sup>96</sup> Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6).

<sup>97</sup> Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

		— Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC <sup>(98)</sup>
	(d) Road	<p>— Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 <sup>(99)</sup> responsible for traffic management control</p> <p>— Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU <sup>(100)</sup></p>
3. Banking		Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 <sup>(101)</sup>
4. Financial market infrastructures		<p>— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU <sup>(102)</sup></p> <p>— Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012 <sup>(103)</sup></p>

<sup>98</sup> Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10)

<sup>99</sup> Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

<sup>100</sup> Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

<sup>101</sup> Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

<sup>102</sup> Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

<sup>103</sup> Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

5. Health		Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU <sup>(104)</sup>
		EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health <sup>105</sup>
		Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC <sup>(106)</sup> Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 Entities manufacturing medical devices considered as critical during a public health emergency ('the public health emergency critical devices list') referred to in Article 20 of Regulation XXXX <sup>107</sup>
6. Drinking water		Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC <sup>(108)</sup> but

<sup>104</sup> Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

<sup>105</sup> [Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted]

<sup>106</sup> Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67).

<sup>107</sup> [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]

<sup>108</sup> Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

		excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential or important services
7. Waste water		Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC ( <sup>109</sup> )
8. Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers
		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		Content delivery network providers
		— Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014( <sup>110</sup> )
		— Providers of public electronic communications networks referred to in

<sup>109</sup> Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p.40).

<sup>110</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73).

		point (8) of Article 2 of Directive (EU) 2018/1972 <sup>(11)</sup> 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
		managed security service providers
9. Public administration		Public administration entities of central governments
		Public administration entities of regional and local governments <sup>(12)</sup>
10. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972

<sup>111</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).

<sup>112</sup> Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).

## ANNEX II

### **IMPORTANT ENTITIES:**

#### ***Sectors, subsectors and types of entities***

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC <sup>(113)</sup> and providers of courier services
2. Waste management		Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC <sup>(114)</sup> but excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture, production and distribution of substances and articles referred to in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 <sup>(115)</sup>
4. Food production, processing and distribution		Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 <sup>(116)</sup>

<sup>113</sup> Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14).

<sup>114</sup> Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)

<sup>115</sup> Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

<sup>116</sup> Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).

5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745 <sup>(117)</sup> , and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 <sup>(118)</sup> with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		— Providers of online marketplaces

<sup>117</sup> Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1)

<sup>118</sup> Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p.176)

		— Providers of online search engines
		— Providers of social networking services platform
7. Education and Research		Higher education institutions and research institutions and their underlying network and information systems

REFERENCE TEXT	AMENDMENT PROPOSAL	RATIONALE
Article 2 <i>Scope</i>		
1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC	1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as <b>medium</b> , micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC	As it stands, the application of the size-cap rule would potentially generate an exponential growth of the entities falling within the scope of the Directive. This would imply that several “new” entities with a different cybersecurity maturity level will have to invest significant resources or, in other terms, bear additional costs for complying with the Directive obligations. The above considerations underlie our proposed new art. 33a (see below). In addition, the exponential growth of the number of entities would significantly impact on the capacity of national competent authorities as well as CSIRTs to carry out the tasks foreseen by the Directive. The former would be demanded of the supervision of several entities as well as of the enforcement of the Directive’s provisions vis-à-vis these entities. The latter would be required to handle a potential huge number of incidents notifications (needless to say about cyber-threats if these are

		covered by the Directive). The above could compromise the capacity of the national competent authority and the CSIRT to carry out their tasks in an effective manner. Therefore, we propose to limit the scope of the Directive to large entities only. Medium, small and micro entities could be covered by the directive only on voluntary basis (see the next amendment below)
2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where	2. However, regardless of their size, <b>this Directive may also be gradually applied, according to specific relevant preconditions established by Member States,</b> <del>also applies</del> to entities referred to in Annexes I and II, where	We propose to leave to the MS the decision on which medium, small and micro entities, and the public administration, include in the scope of the Directive. The inclusion should occur progressively.  In order to avoid that the gradual application of the Directive would result in an excessive exercise of discretionary powers by Member States, we propose to specify that they should identify specific preconditions.
(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;		
(b) the entity is a public administration entity as defined in point 23 of Article 4;	Please, see co-signed non-paper.	Please, see co-signed non-paper
(c) the entity is the sole provider of a service in a Member State;		
(d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;		

(e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;		
(f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;		
(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council <sup>29</sup> [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.	<del>(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council<sup>29</sup> [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.</del>	We suggest to remove the paragraph from this article and include it in a new provision. See below.
Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.	Member States shall establish a list of entities identified pursuant to points (b) to (f) <del>and submit it to the Commission by [6 months after the transposition deadline].</del> <del>Member States shall, review it the list,</del> on a regular basis, and at least every two years thereafter and, where appropriate, update it. <b>The list should be submitted to the Commission by [6 months after the transposition deadline]</b>	The submission of the list to the European Commission should not be an obligation. Member States should not submit the list if national security considerations require not to do so.
	<b>2(a) However, regardless of their size, this Directive also applies to entities referred to in Annexes I, where they are identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.</b>	This provision should ensure that critical entities or entities equivalent to a critical entity will be covered by the provision of NIS regardless of their size.
3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.	Please, see co-signed non-paper.	Please, see co-signed non-paper.

<p>4. This Directive applies without prejudice to Council Directive 2008/114/EC<sup>30</sup> and Directives 2011/93/EU<sup>31</sup> and 2013/40/EU<sup>32</sup> of the European Parliament and of the Council.</p>		
<p>5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities</p>		
<p>6. 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</p>	<p>6. Where provisions of sector-specific <b>Union legal</b> acts of <del>Union law</del> require essential or important entities either to adopt cybersecurity risk management measures or to notify <b>significant</b> incidents <del>or significant cyber threats</del>, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VI, shall not apply <b>to those entities.</b></p> <p><b>In order to ensure a consistent cybersecurity framework, sector-specific legal acts should include, as a minimum standard, cybersecurity risk management measures, and incident notification requirements that reflect those laid down by this Directive.</b></p>	<p><i>[See also the contribution provided with regard to the compromise text drafted by the Portuguese Presidency].</i> It is 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.</p> <p>A clearer approach could entail to refer to the NIS 2 Directive provisions on cybersecurity risk management measures and reporting obligations – as well as supervision and enforcement – as minimum standard for sectorial legislation</p> <p>We believe the notification</p>

		requirement should not include cyber threats.
	<b>7. The Commission should regularly assess the application of the equivalent effect referred in the above paragraph 6 in relation to sector-specific provisions of Union legal acts and should issue guidelines in this regard. The Commission should collaborate with the NIS Cooperation Group when preparing the regular assessment and developing the guidelines.</b>	In light of the considerations made above, we propose to add a new paragraph here which clarifies that the Commission and the NIS Cooperation Group can issue guideline to make the “equivalent effect” principle more concrete and effective
<b>Article 17</b> <i>Governance</i>		
1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.		
2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.		
<b>Article 18</b> <i>Cybersecurity risk management measures</i>		
1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network 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.		
<p>2. The measures referred to in paragraph 1 shall include at least the following:</p> <ul style="list-style-type: none"> <li>(a) risk analysis and information system security policies;</li> <li>(b) incident handling (prevention, detection, and response to incidents);</li> <li>(c) business continuity and crisis management;</li> <li>(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;</li> <li>(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;</li> <li>(f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;</li> <li>(g) the use of cryptography and encryption.</li> </ul>	<p>2. The measures referred to in paragraph 1 shall include at least the following:</p> <ul style="list-style-type: none"> <li>(a) risk analysis and information system security policies;</li> <li>(b) incident handling (<b>incidents</b> prevention, detection, <b>and</b> response <b>and recovery to incidents</b>);</li> <li>(c) business continuity, <b>disaster recovery</b> and crisis management;</li> <li>(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;</li> <li>(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;</li> <li>(f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;</li> <li>(g) the use of cryptography and encryption.</li> </ul>	With respect to incident handling the recovery dimension is currently missing.
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.		
4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring the service concerned into compliance.		

5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.		
6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.		
<b>Article 19</b> <i>EU coordinated risk assessments of critical supply chains</i>		
1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.		
2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.		
<b>Article 20</b> <i>Reporting obligations</i>		
1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with		

<p>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 recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.</p>		
<p>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. Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.</p>	<p><del>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. Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.</del></p>	<p>Given the requirement to notify cyber-threats and in light of these latter's broad and open-ended definition, the number of notification will increase dramatically. First, this would imply additional costs and administrative burdens for entities which will have to comply with the notification requirements established by the Directive. Second, a high number of notifications, will likely disrupt the actual capacity of competent authorities or CSIRTS to handle them. The authorities or the CSIRTs will probably be overwhelmed by notifications. Therefore, unless a clear-cut, narrow and exhaustive definition of cyber-threats is given, it seems preferable to delete this provision.</p>
<p>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;</p>		<p>We have some reservation concerning the expressions "substantial operational disruption", "substantial losses". It should be specified what the terms exactly mean and, above-all, what they imply in terms of the notification requirement for the entities. It seems necessary to establish specific/uniform thresholds to qualify and quantify the "substantiality" of an operational disruption (i.e. an implementing act or guidelines issued by the NIS Cooperation Group).</p>

(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.		We have some reservation concerning the expression “considerable material or non-material losses”. to establish specific/uniform and binding thresholds to qualify and quantify a “considerable” material or non-material loss through an ad hoc instruments (i.e. an implementing act or guidelines issued by the NIS Cooperation Group).
4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT: (a) 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;		
(b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;		
(c) a final report not later than one month after the submission of the report under point (a), including at least the following: (i) a detailed description of the incident, its severity and impact; (ii) the type of threat or root cause that likely triggered the incident; (iii) applied and ongoing mitigation measures.		
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).		
5. 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		

<p>feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. 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. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.</p>		
<p>6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.</p>		
<p>7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.</p>		
<p>8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.</p>	<p>8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.</p>	<p>We propose to delete the requirement to notify cyber-threats for the reasons stated above.</p>

9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	9. <b>Twice per year</b> , <del>the single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on significant incidents, cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report</del>	Submitting a summary report on a “monthly basis” seems determining an excessive burden for single point of contacts.
10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents <del>and cyber threats</del> notified in accordance with paragraphs 1 <del>and 2</del> by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]	We propose to delete the requirement to notify cyber-threats for the reasons stated above.
11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).		
<b>Article 21</b> <i>Use of European cybersecurity certification schemes</i>		
1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT		

services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.		
2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.		
3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.	<b><del>3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.</del></b>	This provision is already foreseen by the Regulation 2019/881, therefore it is redundant.
<b>Article 22</b> <i>Standardisation</i>		
1. 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.		
2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be		

covered.		
<b>Article 28</b> <i>General aspects concerning supervision and enforcement</i>		
1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20.		
2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.		
<b>Article 29</b> <i>Supervision and enforcement for essential entities</i>		
1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.		
2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:	2. Member States <del>shall</del> <b>should</b> ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, <del>have the power to subject those entities</del> <b>may resort to one or more of the following:</b>	In line with the explanations received during the reading phase of the Directive NIS 2 in HWPCI, we prefer to make more clear that national competent authorities should decide which activity to carry out, and establish if and how to run it.  In addition, we suggest to remove the possibility of national competent authorities to resort to security scans that , if not further specified, may include penetration tests.
(a) on-site inspections and off-site supervision, including random checks;	(a) on-site inspections and off-site supervision, including random checks;	
(b) regular audits;	(b) regular audits;	
(c) targeted security audits based on risk assessments or risk-related available information;	(c) targeted security audits based on risk assessments or risk-related available information;	
(d) security scans based on objective, non-discriminatory, fair and transparent risk	<del>(d) security scans based on</del>	

<p>assessment criteria;  (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);  (f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;  (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.</p>	<p><del>objective, non-discriminatory, fair and transparent risk assessment criteria;</del>  (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);  (f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;  (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.</p>	
<p>3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.</p>		
<p>4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:</p> <p>(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;  (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;  (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;  (d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;  (e) order those entities to inform the natural or legal person(s) to</p>	<p>4. Member States <del>shall</del> <b>should</b> ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, <del>have the power to</del> <b>may</b>:</p> <p>(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;  (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;  (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;  (d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;  (e) order those entities to inform</p>	<p>We suggest to eliminate reference to the provisions embedding the so-called principle of “naming and shaming”. First, by requiring the entities to make public aspects of non-compliance, authorities could expose them to more risks. Indeed, threat-actors could consider those entities as the most vulnerable, worth of attacks.  Second, the concerned provisions could expose entities to severe reputational damage.  Third, the principle could be contrary to the core values enshrined in to some MSs’ legal orders.</p>

<p>whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;</p> <p>(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;</p> <p>(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;</p> <p>(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;</p> <p>(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;</p> <p>(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.</p>	<p>the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;</p> <p>(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;</p> <p>(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;</p> <p><del>(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;</del></p> <p><del>(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;</del></p> <p>(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.</p>	
<p>5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:</p>	<p>5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States <b>shall</b> <b>should</b> ensure that the competent authorities <del>have the power to</del></p>	<p>We prefer to make more clear that national competent authorities should decide which measure to adopt</p>

<p>(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;</p> <p>(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.</p> <p>These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.</p>	<p><b>may:</b></p> <p>(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;</p> <p>(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.</p> <p>These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied</p>	
<p>6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive.</p> <p>Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.</p>		
<p>7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:</p> <p>(a) the seriousness of the infringement and the importance of the provisions breached.</p>		

<p>Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.</p> <p>(b) the duration of the infringement, including the element of repeated infringements;</p> <p>(c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;</p> <p>(d) the intentional or negligent character of the infringement;</p> <p>(e) measures taken by the entity to prevent or mitigate the damage and/or losses;</p> <p>(f) adherence to approved codes of conduct or approved certification mechanisms;</p> <p>(g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.</p>		
<p>8. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.</p>		

<p>9. 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 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.</p>		
<p><b>Article 30</b> <i>Supervision and enforcement for important entities</i></p>		
<p>1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures.</p>		
<p>2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to:</p> <ul style="list-style-type: none"> <li>(a) on-site inspections and off-site ex post supervision;</li> <li>(b) targeted security audits based on risk assessments or risk-related available information;</li> <li>(c) security scans based on objective, fair and transparent risk assessment criteria;</li> <li>(d) requests for any information necessary to assess ex-post the</li> </ul>	<p>2. Member States <del>shall</del> <b>should</b> ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, <del>have the power to subject those entities</del> <b>may resort to one or more of the following:</b></p> <ul style="list-style-type: none"> <li>(a) on-site inspections and off-site ex post supervision;</li> <li>(b) targeted security audits based on risk assessments or risk-related available information;</li> <li><del>(c) security scans based on objective, fair and transparent risk assessment criteria;</del></li> </ul>	<p>The proposed amendment reflects the one suggested supra, with regard to essential entities.</p>

cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2); (e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.	(d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2); (e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.	
3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.		
4. Member States shall ensure that the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to: (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive; (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive; (c) order those entities to cease conduct that is in non-compliance with the obligations laid down in this Directive and desist from repeating that conduct; (d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period; (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat; (f) order those entities to	4. Member States <del>shall</del> <b>should</b> ensure that the competent authorities, where exercising their enforcement powers in relation to important entities, <del>have the power to</del> <b>may</b> : (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive; (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive; (c) order those entities to cease conduct that is in non-compliance with the obligations laid down in this Directive and desist from repeating that conduct; (d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period; (e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat; (f) order those entities to	The proposed amendment reflects the one suggested supra, with regard to essential entities.

<p>implement the recommendations provided as a result of a security audit within a reasonable deadline;</p> <p>(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;</p> <p>(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;</p> <p>(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.</p>	<p>implement the recommendations provided as a result of a security audit within a reasonable deadline;</p> <p><del>(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;</del></p> <p><del>(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;</del></p> <p>(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.</p>	
<p>5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for the important entities listed in Annex II.</p>		
<p><b>Article 31</b></p> <p><i>General conditions for imposing administrative fines on essential and important entities</i></p>		
<p>1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.</p>		
<p>2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).</p>		

3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7).		
4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.	<del>4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.</del>	We think the amount of administrative fines should be decided by Member States and established by National law.
5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.		
6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.		
<b>Article 32</b> <i>Infringements entailing a personal data breach</i>		
1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of		

that Regulation within a reasonable period of time.		
2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58(i) of that Regulation and impose an administrative fine, the competent authorities shall not impose an administrative fine for the same infringement under Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive.		
3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority may inform the supervisory authority established in the same Member State.		
<b>Article 33</b> <i>Penalties</i>		
1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.		
2. Member States shall, by [two] years following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.		

	<b>NEW ARTICLE:</b> <b>33a</b> <b>To sustain and foster compliance with the obligations laid down by this Directive, in particular with the cybersecurity risk management measures and the reporting requirements, essential and important entities may have access to appropriate European Funding Schemes.</b>	We think the Directive should refer explicitly to the possibility that essential and important entities may have access to EU funding schemes in order to support the implementation of the measures established by the Directive and comply with its obligations. In particular, this could encourage and help entities to adopt cybersecurity risk management measures and comply with the reporting obligations.
<b>ANNEX I</b> <b><i>ESSENTIAL ENTITIES</i></b>		<b>COMMENTS</b>
1. Energy (a) Electricity (b) District heating and cooling (c) Oil (d) Gas (e) Hydrogen		
2. Transport (a) Air (b) Rail (c) Water (d) Road	2. Transport (a) Air (b) Rail (c) Water (d) Road <b>(e) mass transit</b>	Given the importance of the sub-sector in terms of the provision of essential services for the society and economy, we propose the inclusion of the so-called “mass transit” systems (e.g. tram, metro, bus) under the scope of the Directive.
3. Banking		
4. Financial market infrastructures		
5. Health		
6. Drinking water		
7. Waste water		

8. Digital infrastructure		
9. Public administration		
10. Space		
<b>ANNEX II</b> <b><i>IMPORTANT ENTITIES</i></b>		
1. Postal and courier services		
2. Waste management		
3. Manufacture, production and distribution of chemicals		
4. Food production, processing and distribution		
5. Manufacturing (a) Manufacture of medical devices and in vitro diagnostic medical devices; (b) Manufacture of computer, electronic and optical products (c) Manufacture of electrical equipment (d) Manufacture of machinery and equipment n.e.c. (e) Manufacture of motor vehicles, trailers and semi-trailers (f) Manufacture of other transport equipment		

6. Digital providers		
----------------------	--	--

PUBLIC

## NETHERLANDS

### Additional drafting proposals by the Netherlands regarding the interplay between NIS

24 June 2021

*(Article 2 and Annexes, and Articles 17-22, 28-33)*

Disclaimer: this list of drafting proposals is an initial compilation of suggested amendments from the Netherlands at this point in time. The list of amendments is preliminary and can be expanded or adjusted in the future and does not represent a final position from the Netherlands on the articles covered in this round of proposals.

Art.	Commission proposal	Drafting proposal	Motivation
Annex I & 2		Study reservation	<p>As mentioned in our written and oral questions during the readthrough, the Netherlands has concerns regarding the proportionality of the proposal. The combination of article 2 and the extension of the sectors listed in annex I &amp; II leads to a significant increase in the amount of entities in scope of the Directive, which has serious consequences for the administrative burden for entities and authorities.</p> <p>While we understand the need to critically assess the scope of the Directive, the Netherlands is of the opinion that regulation of additional sectors, subsectors and entities can only take place after a risk assessment has established that this is proportional</p>

			<p>to the objective of this Directive. The Netherlands considers it necessary to have a substantive discussion on the sectors, subsectors and the definition of the type of entities covered in Annex I &amp; II. It is crucial that the scope of this Directive is risk based, and the annexes should reflect this.</p> <p>Additionally, the Netherlands will submit a non-paper on article 2 simultaneously with these drafting proposals (see below).</p>
2			The Netherlands will submit a non-paper on article 2 simultaneously with these drafting proposals. The proposals from this paper could be processed into drafting proposals after an initial discussion.
2			The Netherlands supports the non-paper drafted by Poland on the inclusion of public administration in the NIS Directive framework, including the drafting proposals.
2 (2)	Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.	Member States shall establish a list of entities identified pursuant to points (b) to (f) <b>and submit it to the Commission by [6 months after the transposition deadline]</b> . Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.	<ul style="list-style-type: none"> <li>• The added value of this reporting obligation is unclear.</li> <li>• Moreover, information on (some of the) entities that will be covered by points (b) and (f) is confidential from the perspective of national security, which is not acceptable.</li> </ul>
2 (3)	This Directive is without prejudice to the	This Directive is without prejudice to the <b>responsibility</b> competences of Member States	<ul style="list-style-type: none"> <li>• In order to better align this article with the text of the TEU.</li> </ul>

	competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.	<del>concerning the maintenance of</del> <b>regarding essential State functions including</b> public security, defence and national security <b>in accordance</b> <del>in compliance with Union law.”)</del>	
2 (6)	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.	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 <del>significant cyber threats</del> , and where those requirements <b>in combination with the supervision thereon and enforcement thereof</b> 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.	<ul style="list-style-type: none"> <li>• We think that it important that also the supervision and the enforcement of the sector-specific acts of Union law should be at least equivalent in effect. Otherwise, the security and notification requirements can be the same in effect, but the total effectiveness of the sector-specific act may not, due to lacking possibilities in supervision and enforcement.</li> <li>• Deletion of cyber threats in order to align with the amendment of art. 20 (2)</li> </ul>
17 (1)	Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.	Member States shall ensure that the management <del>bodies</del> of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18 <b>and supervise oversee</b> its implementation <b>and operating effectiveness</b> <del>and be accountable for the non-compliance by the entities with the obligations under this Article.</del>	<ul style="list-style-type: none"> <li>• It is important that management bodies are aware and take responsibility for cybersecurity risk management measures.</li> <li>• However, this article in combination with art. 29 (6) opens up the possibility of liability of natural persons in management bodies. The Netherlands considers the introduction of liability of natural persons for compliance with the obligations from this Directive as disproportional to the intended objective of this article. The Netherlands is still exploring</li> </ul>

			<p>whether there are objections from a legal perspective to this inclusion as well.</p> <ul style="list-style-type: none"> <li>• Instead, the Netherlands proposes to make the assignment of cybersecurity responsibilities to existing management layers part of the cybersecurity risk management measures in art. 18. See our proposal below.</li> <li>• The term 'supervision' should be reserved for competent authorities</li> <li>• Furthermore, we believe that it is important that also the effectiveness of measures is taken into account, as is usual in IT-auditing including risk management.</li> <li>• We believe that "bodies" in "management bodies" is redundant.</li> </ul>
<b>Art. 17 (2)</b>	Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.	<del>Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.</del>	<ul style="list-style-type: none"> <li>• Developing awareness and skills within management bodies is a laudable goal, but it would be micro management and disproportional to make this obligatory through this Directive.</li> <li>•</li> </ul>

Art. 18 (1)	Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network 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.	<i>The Netherlands would welcome drafting proposals to further define "their services"</i>	<ul style="list-style-type: none"> <li>• The Netherlands is concerned that the current proposal is too broad in defining the services within an entity to which the risk management measures should apply.</li> <li>• Entities can provide many different services, not all of which should be considered essential or important from the perspective of this Directive.</li> <li>• NIS1 focused on the operators of essential services (OES) but these OES were subject to the specific security requirements only with respect to those services which are deemed to be essential. This ensures that entities that provide both essential and non-essential entities focus their efforts and investments concerning cybersecurity mainly on those processes that are deemed essential or important.</li> <li>• The proposed text creates uncertainty for entities as well as authorities on the scope of the security requirements. The objective of the NIS2 should be to protect the essential and important services that entities provide.</li> <li>• Further discussion on this would be needed.</li> </ul>
18 (2) d	supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as	supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers <del>such as providers of data storage and processing services or managed security services;</del>	<ul style="list-style-type: none"> <li>• As mentioned above, the current wording creates uncertainty for entities as well as authorities regarding the scope of the suppliers that should be understood to be covered by the security</li> </ul>

	providers of data storage and processing services or managed security services;	<i>The Netherlands would welcome drafting proposals to further define the services to which this section would apply.</i>	<p>requirements.</p> <ul style="list-style-type: none"> <li>• This is especially the case in this section. Entities can have many suppliers, not all of which are relevant from the perspective of this Directive. It should be clear that suppliers of the company restaurant or office supplies are out of scope.</li> <li>• Additionally, in line with other articles and paragraphs of the proposal, we think it is not necessary to provide these details and examples in this subparagraph. Alternatively, these examples could be made explicit in a recital.</li> </ul>
18 (2) g	(g) the use of cryptography and encryption.	(g) the use of cryptography and encryption, <b>including cryptographic key management and digital signatures</b>	In taking appropriate measures regarding the use of cryptography and encryption, it should be clear that this includes cryptographic key management and digital signatures.
18 (2) h	[addition]	<b>(h) assignment of cybersecurity responsibilities to intermediate management layers</b>	<ul style="list-style-type: none"> <li>• A policy for assigning cybersecurity measures is missing in the current proposal.</li> <li>• Operational and day-to-day cybersecurity affairs should be assigned in existing management layers of an organisation, which should be supported by a CISO and fall under the final responsibility of higher management.</li> <li>• Incidents can occur in an organisation because there is no clear ownership in intermediate layers. It requires adopting policies</li> </ul>

			<p>to avoid such incidents.</p> <ul style="list-style-type: none"> <li>Furthermore, it is in line with the overall focus in NIS2 to be specific about responsibilities (example art. 29 (4) ). This amendment contributes to the overall aim to assign responsibilities at the appropriate levels.</li> </ul>
18 (6)	<p>The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.</p>	<p><del>The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.</del></p>	<ul style="list-style-type: none"> <li>The Netherlands is of the opinion that this covers essential parts of legislation and as a consequence, is not suitable for delegated acts.</li> </ul>
20 (1)	<p>Member States shall ensure that essential and important entities 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 recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent</p>	<p>Member States shall ensure that essential and important entities 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 <b>and within reason</b>, those entities shall notify, without undue delay, the recipients of their services of <b>these</b> incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.</p> <p><i>The Netherlands would welcome drafting proposals to further define "their services"</i></p>	<ul style="list-style-type: none"> <li>As mentioned in our comments on article 18, the current wording in relation to "their services" creates uncertainty for entities as well as authorities regarding which incidents should be notified. This could lead to unnecessary administrative burden and a surge in notifications that are not relevant from the perspective of this Directive for authorities.</li> <li>Addition of "these" in order to make clear that the notification to recipients considers the same incidents as mentioned in the first sentence of this section.</li> <li>Additionally, it should be clear that it is not always possible or helpful to inform recipients of a service of an incident.</li> </ul>

	authorities or the CSIRT to determine any cross-border impact of the incident.		
20 (2)	<p>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. Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.</p>	<p>Member States shall <b>encourage</b> ensure that essential and important entities <b>to</b> 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.</p> <p>Where applicable <b>appropriate</b>, those entities <b>may</b> shall notify, <del>without undue delay</del>, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities <b>may</b> shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.</p>	<ul style="list-style-type: none"> <li>• The obligation to notify authorities of significant cyber threats to the CSIRT was already part of existing (national) legislation in the Netherlands. After nearly three years, this obligation has not resulted in a better situational awareness for CSIRTs.</li> <li>• In addition, there is a reasonable fear that this could lead to an overwhelming amount of additional notifications because entities are incentivized to notify irrelevant situations in their desire to be compliant (better safe than sorry).</li> <li>• For the reasons listed above, the Netherlands believes that it would be more beneficial to promote the voluntary notification of cyber threats and the exchange of relevant threat information through information sharing arrangements (through article 26).</li> <li>• Considering that this article relates to the reporting obligations, it might be necessary to move this section to a separate article.</li> </ul>
20 (3)			•
20 (9)	The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses	The single point of contact shall submit to ENISA <del>on a monthly basis</del> <b>an annual</b> summary report including anonymised and aggregated data on incidents, <del>significant cyber threats and near misses</del> notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA	<ul style="list-style-type: none"> <li>• This extended reporting obligation for the single point of contact is not proportional to the interest of having more frequent summary reports</li> <li>• Deletion of cyber threats and near misses in order to align this article with the drafting proposal of art. 20 (2)</li> </ul>

	notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	may issue technical guidance on the parameters of the information included in the summary report.	
<b>20 (10)</b>	Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents <del>and cyber threats</del> notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	<ul style="list-style-type: none"> <li>• Deletion of cyber threats and near misses in order to align this article with the drafting proposal for art. 20 (2)</li> </ul>
<b>20 (11)</b>	The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as	The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. <del>The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).</del>	<ul style="list-style-type: none"> <li>• The Netherlands is of the opinion that this covers essential parts of legislation and as a consequence, is not suitable for implementing acts.</li> </ul>

	referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).		
21		<i>The Netherlands has submitted drafting proposals on this article in its written response (17 June 2021) to the Presidency compromise proposal on interaction of NIS 2 with sectoral legislation. The Netherlands thanks the Presidency for including these drafting proposals in rev 1 of the compromise proposal.</i>	<ul style="list-style-type: none"> <li>• It is desirable to add an option for Member States to require entities to certify ICT products, ICT services and ICT processes to demonstrate a presumption of conformity.</li> <li>• It provides the possibility of a more light touch approach where mandatory certification is not (yet) appropriate and gives the opportunity to ascertain whether a certain certification works in practice for important and essential entities.</li> </ul>
21 (1)	In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.	<p><del>In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.</del></p> <p>a) Member States may provide that essential or important entities can 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 to establish a presumption of conformity with certain requirements of Article 18. The products,</p>	<p>For the sake of clarity and to prevent renumbering, we have used 21-1 (a) and (b), but in the final legal text, parts of article 21 could be renumbered to 21-1 (proposed 21-1(a), 21-2 (proposed 21-1(b) and 23-3 (proposed 21-2).</p> <p>Our proposal creates an additional option besides the original one in the Commission proposal. The proposed (b) corresponds with the original proposal of the Commission, but it has been rewritten to have the same syntax as (a), where we introduced a new option. Under (a), Member States do not require entities to certify, but when they do, they get the advantage that it is presumed that they are compliant with certain aspects of article 18 where the specific certification is geared towards.</p>

		<p>services and processes subject to certification may be developed by an essential or important entity or procured from third parties.</p> <p>b) Member States may provide that that essential or important entities are required to certify certain ICT products, ICT services and ICT processes under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 to demonstrate conformity with certain requirements of Article 18. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.</p>	<p>Hereby Member States can incentivize instead of obligate entities to certify, creating in effect a testing ground to see whether the market adopts the certification and it works as expected. Based on those experiences, Member States and mutatis mutandis the Commission can choose to keep that practice, make necessary changes or if necessary make certification mandatory.</p> <p>This option of presumption of conformity is a concept and practice that we borrowed from the European "New Approach" better regulation model and other EU legislation. The idea is that it provides the best of both worlds: you have clear requirements to which a party can certify, but parties can also come up with other ways to conform to the essential requirements as stipulated in the legislation.</p> <p>In 21 (2), we create the same two options in case of a implementing act by the Commission. Here we changed delegated act to implementing act, to give Member States and the EU Parliament a greater say in the adoption process. Also we proposed some additional due diligence on the side of the Commission before proposing the implementing act.</p> <p>In effect our proposal creates the following options for Member States (21-1) and Commission (21-2), in order of the impact they have on entities:</p>
--	--	--	--

			<table><tr><td></td><td><b>Original proposal</b></td><td><b>Our proposal</b></td></tr><tr><td>1</td><td>Voluntary certification by entities (No need to make this explicit in the NIS)</td><td>Voluntary certification by entities (No need to make this explicit in the NIS)</td></tr><tr><td>2</td><td></td><td>Voluntary certification by entities, but with advantages for entities if they do (21-1 (a))</td></tr><tr><td>3</td><td>Mandatory certification (21-1)</td><td>Mandatory certification (21) (b)</td></tr></table>		<b>Original proposal</b>	<b>Our proposal</b>	1	Voluntary certification by entities (No need to make this explicit in the NIS)	Voluntary certification by entities (No need to make this explicit in the NIS)	2		Voluntary certification by entities, but with advantages for entities if they do (21-1 (a))	3	Mandatory certification (21-1)	Mandatory certification (21) (b)
	<b>Original proposal</b>	<b>Our proposal</b>													
1	Voluntary certification by entities (No need to make this explicit in the NIS)	Voluntary certification by entities (No need to make this explicit in the NIS)													
2		Voluntary certification by entities, but with advantages for entities if they do (21-1 (a))													
3	Mandatory certification (21-1)	Mandatory certification (21) (b)													
21 (2)	<p>The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.</p> <p><i>Presidency compromise text:</i> The Commission shall be</p>	<p><del>The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.</del></p> <p>The Commission shall be empowered to adopt implementing acts specifying which categories of essential entities can demonstrate a presumption of conformity or are required to demonstrate conformity with certain requirements of Article 18, by certifying certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to</p>	<p>More clarity in article 21 (2) could be provided by formulating it separately from 21 (1). Furthermore, also in this case the option of presumption of conformity would be advantageous, as in 21(1). Last, due diligence on the consequences of certification should be part of the process, following the example of article 56 (2) of regulation (EU) 2019/881.</p> <p>Furthermore, we would propose to use the mechanism of implementing acts with the examination procedure.</p>												

	<p>empowered to adopt delegated acts specifying which categories of essential entities shall be required <b>to use certain certified ICT products, ICT services and ICT processes</b> or obtain a certificate and under which specific European cybersecurity certification schemes <b>adopted pursuant to Article 49 of Regulation (EU) 2019/881</b>. pursuant to paragraph 1The delegated acts shall be adopted in accordance with Article 36.</p>	<p>Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential entity or procured from third parties. When preparing the implementing act, the Commission shall:</p> <ul style="list-style-type: none"> <li>(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services or ICT processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services or ICT processes;</li> <li>(b) take into account the existence and implementation of relevant Member State and third country law;</li> <li>(c) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;</li> <li>(d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services or ICT processes, including SMEs;</li> </ul>	
<b>21 (3)</b>	<p>The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European</p>	<p>The Commission may request ENISA to prepare a candidate scheme <b>or to review an existing European cybersecurity certification scheme</b> pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.</p>	<ul style="list-style-type: none"> <li>• The NIS2 could lead to new requirements that could fit within existing certification schemes. Adding the option to review existing schemes would help in this situation.</li> </ul>

	cybersecurity certification scheme for the purposes of paragraph 2 is available.		
		<i>In comparison to NIS 1, the authorities for supervision and enforcement that Member States should create in their national legislation have been significantly expanded in the proposal for NIS 2. As a general comment related to Chapter IV, the Netherlands might follow up with additional comments and suggestions in a later phase.</i>	•
29 (2)	Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:	Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities <b>at least</b> to: [...]	• This makes explicit that Member States should be able to grant additional powers to the competent authority.
29 (4) e	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of <b>the nature of the threat, as well as</b> of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	<ul style="list-style-type: none"> <li>• Organizations are responsible for choosing their own security measures, based on a risk analysis (i.e. risk management). In order to do so, they need information on the nature of the threats against which they are trying to protect themselves.</li> <li>• The service provider (i.e. the essential entity) does not have sufficient insight into or knowledge of the threat profile of the service consumer (i.e. the natural or legal person) to make this assessment by itself.</li> <li>• Therefore, it should be possible for Member States to order essential entities to disclose the nature of the threat that service providers (and therefore indirectly, the service</li> </ul>

29 (5) b	impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.	<del>impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.</del>	customers themselves) are facing. <ul style="list-style-type: none"> <li>As mentioned in our comments under article 17 and below, the Netherlands considers the introduction of liability of natural persons for compliance with the obligations from this Directive as disproportional to the intended objective of this article. The Netherlands is still exploring whether there are objections from a legal perspective to this inclusion as well.</li> </ul>
29 (6)	Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.	<del>Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.</del>	<ul style="list-style-type: none"> <li>The Netherlands considers the introduction of liability of natural persons for compliance with the obligations from this Directive as disproportional.</li> </ul>
29 (7) c	(c) the actual damage	(c) the actual damage caused or losses	<ul style="list-style-type: none"> <li>People's lives are important, even if</li> </ul>

	caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;	incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of <b>the risk of actual or potential loss of life and physical, social, emotional and psychological well-being</b> , actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;	they are not users of the specific essential entity whose cybersecurity was impacted. The current text only considers the impact of an incident on the users of the essential entity, not other people. This addition provides at least a modicum of consideration for the people who are affected, but who are not users of the essential entity. An example would be the people whose health is in danger when a cybersecurity incident at a chemical plant leads to the release of toxic fumes into the air they breathe. Physical, social, emotional and psychological well-being is included in line with SSVC's assessment of safety impact ( <a href="https://raw.githubusercontent.com/CERTCC/SSVC/main/doc/pdfs/2021_019_001_653461.pdf">https://raw.githubusercontent.com/CERTCC/SSVC/main/doc/pdfs/2021_019_001_653461.pdf</a> )
29, 30		<i>The Netherlands is not convinced whether it is necessary to have separate articles to lay down the authorities for supervision and enforcement for essential as well as important entities. These authorities might also be covered in a single article, in order to provide more legal clarity.</i>	
30 (2)	Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to: (a) on-site inspections and off-site ex post supervision; (b) targeted security audits	Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities <b>at least</b> to: (a) on-site inspections and off-site ex post supervision; (b) targeted security audits based on risk assessments or risk-related available information; (c) security scans based on objective, fair and transparent risk assessment criteria;	<ul style="list-style-type: none"> <li>• This makes explicit that Member States should be able to grant additional powers to the competent authority.</li> <li>• Furthermore, it should be possible to request evidence of implementation of cybersecurity policies of important entities.</li> </ul>

	<p>based on risk assessments or risk-related available information;</p> <p>(c) security scans based on objective, fair and transparent risk assessment criteria;</p> <p>(d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);</p> <p>(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks</p>	<p>(d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);</p> <p>(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks</p> <p><b>(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.</b></p>	
<b>30 (2) f</b>	[addition]	<b>requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.</b>	<ul style="list-style-type: none"> <li>• Addition in order to align this article with the authorities of competent authorities under art. 29 (2)</li> </ul>
<b>30 (3)</b>	Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	Where exercising their powers pursuant to points (d) <del>or to</del> (e f) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	<ul style="list-style-type: none"> <li>• Amendment in order to align this article with the suggested amendment of article 30 (2)</li> </ul>
<b>31 (4)</b>	Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with	Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least	<ul style="list-style-type: none"> <li>• The lower limit for the fine maximum is 10 million euros. As a percentage of total worldwide annual turnover, it should be 2%. However, the current phrasing</li> </ul>

	paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.	10 000 000 EUR or <del>up to</del> 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.	seems to allow the Member States to set a lower percentage. This change attempts to clarify the situation.
32		<i>The Netherlands would welcome suggestions to make the provisions in this article for the cooperation between competent authorities and data protection authorities more reciprocal</i>	
33 (2)	Member States shall, by [two] years following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.	<del>Member States shall, by [two] years following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.</del>	The objective of this reporting obligation is unclear. The drafting and implementation of rules and measures regarding supervision and enforcement is the prerogative of the Member States.
Annex I, 1 (a)	[addition]	1. Energy (a) Electricity [...] - <b>Delegated operators referred to in point (33) of Article 2 of Directive (EU) 2019/943</b> - <b>Balance responsible party referred in point (14) of Article 2 of Regulation (EU) 2019/943;</b> - <b>Operators that at a distance by electronic means can change, intentionally or not, the electricity load or generation by final customers or producers from their normal</b>	Delegated operators should be included, so that also entities to whom specific tasks or obligations entrusted to a transmission system operator or nominated electricity market operator under this Regulation or other Union legal acts have been delegated by that transmission system operator or NEMO or have been assigned by a Member State or regulatory authority will fall within the scope of the directive. Otherwise, essential services could fall

		<p><b>or current consumption or production patterns leading to a risk of electricity grid instability.</b></p>	<p>out of scope, since the annex is based on types of entities.</p> <p>Balance responsible parties are important for balancing the electricity system and should therefore be included.</p> <p>Furthermore, there are more and more parties that through the internet can influence the consumption or production of electricity by final customers and producers. Think of manufacturers of solar invertors that remotely can influence or disable converters. Or think of charge point operators for electronic vehicles, manufacturers of electric vehicles and manufacturers of heat pumps that can do the same for their devices. Because these devices are more and more connected through the internet of things, such manufacturers in total control a huge amount of electric load or production, posing significant danger to grid stability. Not all of these parties fall under the definition of "aggregator" or "demand response" of Directive (EU) 2019/944. Often, they have the technical capability to influence the devices, but they are not active electricity market participants. Also, more and more production sites are remotely controlled by operators that operate multiple sites as a service. We therefore think these aforementioned entities should be included separately.</p>
--	--	--	--

## SPAIN

### Article 2. Scope

#### AMMENDMENT 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

**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.”**

### **AMMENDMENT 3**

#### **The biennial revision of the list of entities identified by MS should be annual**

Article 2 states that: “*Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.*” We suggest that this revision should be annual in order to account for the high variability of the market.

### **AMMENDMENT 4**

#### **Reinforce the supervision of the supply chain**

In line with recital 1, the scope of article 2 should be broadened to include those technological providers that represent a risk in the supply chain. Entities in the scope of NIS should identify these providers when performing their risk analysis and declare them to the MS competent authorities.

In line with recital 2 according to assessment of the supply chain, following the same model of EU recommendations for a certain sector (e.g. *Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group*), supply chain or technology, it would be needed to progress in the elaboration of a set of recommendations or toolbox for IoT. This technology is increasingly present in more contexts and services are starting to become dependent of it, exactly as in the case of 5G.

### **Article 4 Definitions**

### **AMMENDMENT 5**

(5) ‘incident’ means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;

**Proposal:** It does not define “near miss” although it is a concept that it uses later.

It is proposed that it incorporate the definition of “near miss” as (5a) ‘near miss’ means an event which could have caused harm, but was successfully prevented from fully transpiring.

(6) ‘incident handling’ means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;

Continuity of activities or crisis management is not defined, although they are mentioned in article 18 as measures to be carried out by essential and important organizations.

**Proposal: define crisis and crisis management.**

## Article 17 Governance

### AMMENDMENT 6

2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.

***Comment: Very important article because it emphasizes the need for the involvement and commitment of the management, for which it is essential that they know and understand the dimension of risk.***

***A change is proposed: that the members of the management bodies do NOT have to evaluate cybersecurity risks, they are not trained to evaluate, but they have to know and understand the risks and consequently have to approve the level of risk and the controls that are in place. carrying out as a company.***

***It is proposed to include in the report to the administration that such training and training has been carried out for the management bodies.***

## Article 18 Cybersecurity risk management measures

### AMMENDMENT 7

We strongly request that in paragraphs 18.5 and 18.6, where it says that "The Commission may adopt implementing acts" this is substituted by "**The Commission SHALL adopt implementing acts**". And that an explicit deadline for these implementing acts is included.

#### **JUSTIFICATION**

The measures indicated in paragraph 18.2 of Article 18 of the proposed revision of the NIS Directive broadly follow the spirit and letter of Article 2 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

The Supervisory Bodies' experience with the aforementioned Article 2 has been negative. It outlines broadly the elements of ICT Security standards, but it is too undefined to enforce even the smallest level of compliance with any ICT standard. This explicitly harmed supervision efforts, giving supervised entities a way out as long as they included the listed elements, as unsatisfactory as they may have been. It also created a de facto legal heterogeneity, as every MS's Supervisory Body interpreted Article 2 differently.

### AMMENDMENT 8

2. The measures referred to in paragraph 1 shall include at least the following:

**Proposal 1:** It is proposed to include an additional measure: Training and training of management.

## **Proposal 2:**

...// (c) business continuity and crisis management; //...

Many companies that have business continuity in place (with or without a management system) have included activities that are critical to the business but perhaps not for the purposes of the system / country. It is proposed that "continuity of activities" be more concrete and / or explicit and that it refers to or mentions essential activities, those that support essential services.

It is believed appropriate to introduce criteria to identify what is essential and critical so as not to transfer the decision of what is essential to companies only (in the statement of applicability).

In this sense, it is considered necessary to expand the explanations on the elements or attributes or criteria that can help determine what is critical and therefore, requires that continuity measures be developed as mentioned in this article. Criteria should include impact criteria (which leads to a BIA analysis) and recovery time criteria (which provides a RTO analysis).

In this point; the need to validate potential overlap with the Resilience Directive, which is also in process, was confirmed).

Expand / specify the activities that had to fall under the requirement of the "continuity of activities" measure, including criteria for companies so that they consider the continuity of essential services for the country.

These criteria would help to limit later, what would be mandatory to notify.

Regarding crisis management: it is proposed to include as a minimum:

- Crisis management plan with action procedure, Crisis Committee with responsibilities and roles, activation criteria.

## **AMMENDMENT 9**

It is also recommended that art. 18.2 be enriched with the provisions of Spanish Royal decree law 12/2018. In RD Development of RDL 12/2018, the following are listed as minimum measures:

- a) Risk analysis and management.
- b) Risk management of third parties or suppliers
- c) Catalog of security, organizational, technological and physical measures.
- d) Management and professionalism of personnel.
- e) Acquisition of security products or services.
- f) Incident detection and management.
- g) Recovery plans and assurance of the continuity of operations

## Article 20. Reporting obligations

### AMMENDMENT 10

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:
  - o ~~... "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" ...

## **AMMENDMENT 11**

*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.*

*Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.*

**Proposal:** A threat means that the damage is potential, and that if it materializes it could cause a significant impact, therefore, it is assumed that it has not yet materialized.

Thus, it is understood that warning of threats can help member states to act preventively. On the contrary, there is a risk of over-reporting threats and causing over-reporting (difficult to handle).

Therefore, and being aware of the preventive value of having information even if the incident has not materialized, it is proposed that criteria be introduced that help to discern which threats are really convenient to be reported obligatorily.

In this sense, it should be noted that in Spain the National Guide already guides reporting based on the classification of the incident according to its taxonomy, its impact and its potential danger, which is important to act preventively.

## **AMMENDMENT 12**

*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.*

*(...)*

*11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).*

**Proposal:** This topic is critical and it seems that it is too "open" for the purposes of what must be notified on a mandatory basis.

There is the risk of generating an excess of notifications, and on the contrary of omitting relevant ones due to the ambiguity of what may be significant-

There is a **need to introduce criteria or levels** that serve to differentiate by levels of severity, impact, even potential danger, and therefore help to limit the size of the volume of notifications (National Guide) and to provide more elements on what has to be done. consider "significant".

Furthermore, for several sectors there are sector-specific considerations, widely established metrics and widely established practices that should be included in the criteria to gauge the severity of their incidents.

Therefore we propose that paragraph 11 of Article 20 is changed as follows, where the date is to be considered to be one year after the enactment of the proposed Directive:

*11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. ~~The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. By 1 December 2022, taking into account relevant sector-specific considerations, metrics and practices and subject to paragraph 3, the Commission shall, by means of implementing acts, further specify the cases, criteria and levels in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).~~*

Otherwise, if the Commission is not ready to adopt this modification, the following paragraph, already extant in the current NIS Directive, shall be added to Article 20:

*Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 3.*

### **AMMENDMENT 13**

*4. Member States shall ensure that, for the purpose of the notification under paragraph*

*1, the entities concerned shall submit to the competent authorities or the CSIRT:*

*(a) 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*

**Proposal:** The usefulness of being notified within 24 hours is verified, and it is considered that this has to be one of the actions / tasks that must be included in the incident management procedure (see media art 18).

However, insist on the need or convenience of greater clarity in the criteria to determine what has to be notified: principle of proportionality.

As an example, if a company is at an emergency or crisis level due to a technological incident, it would have to be a criterion to notify.

On the other hand, in general, there is little bidirectionality of the information, and therefore, there is a path of improvement in this matter. The administration has great potential as an aggregator of information and its return to companies, communication that could result in the improvement of the collective and individual response.

Therefore: **introduce the concept of proportionality**, which is important for the incident itself and for the consequences on the essential service, and explore the possibility of introducing greater reciprocity that serves to alert and assist in management.

### **Article 21 Use of European cybersecurity certification schemes**

#### **AMMENDMENT 14**

The art. 21 (paragraph 2) should be modified to allow the coexistence of European and National frameworks like the ENS-NSF:

<<Article 21. Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.
2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.

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

#### **JUSTIFICATION**

NISD2 proposal should take into consideration the existence of existing national tools that have proven their effectiveness over the years in the field of cybersecurity. This is the case, in Spain, of the National Security Framework (ENS-NSF).

The National Security Framework (ENS-NSF) is especially important because:

1. It is a cybersecurity evaluation and certification scheme regulated by law, approved by the Spanish Parliament in 2010.
2. It applies to the entire Spanish public sector (some 30,000 entities) and also applies to companies providing services to public entities.
3. The number of evaluated and certified entities is several hundred.
4. It is a scheme specifically aimed at ensuring the security of the provision of public services, with all the importance that this entails, with particular impact on Chapter IV Cybersecurity risk management and information obligations, as it provides a common approach to basic principles, minimum requirements, security measures and audit and conformity assessment procedures through the accreditation of certification bodies against the ISO/IEC 17065 standard by the

National Accreditation Body (ENAC), as well as the monitoring of the status of entities within the scope of the ENS.

All these reasons more than justify the need to respect this evaluation and certification scheme, allowing the permanence of the ENS-NSF and its coexistence with the other new schemes that may be implemented in the EU.

## **AMENDMENT 15**

### **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 16**

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

#### Amendment

Sector	Subsector	Type of entity
<b>6a Digital infrastructure</b>		— 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 <b><i>when they qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.</i></b>

## 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.

## GENERAL COMMENTS

<b>Article 2. Scope</b>	<p>Regarding the scope of the future Directive (strategic sectors of essential services), <b>its scope is significantly broadened</b> compared to the one now in force and, in addition, it coincides with the project also underway to review the Directive 2008 / 114, CIP, logical position if it is understood that the purpose of both standards (CIP and NIS) is to protect and guarantee the provision of essential services for society, so it would not make any sense that they were different.</p> <p>This NIS-CIP alignment is good for Spain, due to since 2011 there are <b>12 identified strategic sectors</b> (beyond what is required by European regulations), which are identical for both the CIP legislation (Law 8/2011) and NIS (RD-I 12/2018).</p> <p>Also striking, importantly, is the <b>diametrical change in the methodology provided by NIS 2 to identify “essential” and “important” entities</b>. Thus, it eliminates the identification criteria</p>
-------------------------	---

	<p>in force in the current NIS Directive, based on the concept of <b>"significant disturbing effect"</b>, of a more restrictive nature, and passes to a <b>much more open criterion</b> in which any medium or large company operating in any of the sectors of the annexes of the Directive is now qualified as a taxpayer of the standard. Two conclusions can be drawn from all this:</p> <ul style="list-style-type: none"> <li>- The identification criteria in force in the current NIS Directive are deleted from the draft NIS 2, but are transferred in full to the draft CER Directive. Significantly, it seems to follow that the future "critical entities" of this Directive will be a subsection of the "essential" or "important" ones, based on their higher level of potential impact to these essential services.</li> <li>- The much more open identification criterion of the NIS 2 <b>will represent a huge increase over the currently existing entities</b> (around 200). Considering that in Spain there are more than <b>50,000</b> medium and large companies, the number of entities potentially subject to the future NIS 2 Directive will be several thousand. This will undoubtedly have <b>consequences</b>, both <b>on the security obligations</b> that will be transferred to this type of company, <b>and on the essential increase in management capacity that must be implemented by the competent Spanish Administration</b> to deal with this volume.</li> </ul> <p>There must be a <b>mechanism to classify as "Essential Entity" to "Important Entities"</b> when they have a <b>dominant market position or the interruption of the service that could provide systemic risks</b>. At the very least, their ex ante supervision should be allowed in these cases</p> <p>It should be more clearly defined <b>which entities of the public administrations are within the scope</b> of the proposal and which are not.</p> <p><b>Micro and small companies of communications infrastructure and services operators should be categorized as "Important Entities"</b> instead of "Essential Entities", moving from an ex ante supervision regime to one of ex post supervision.</p> <p><b>Trust services should be eliminated</b> as a subsector of essential entities in application of the principle of <b>lex specialis</b>, as in the current Directive</p> <p>Member States should have <b>margin</b> within their scope to apply the <b>measures</b> provided for in article 2.2 (and those that may arise from the acts provided for in sections 2.5 and 2.6) according to their security frameworks, which in Spain is the National Security Framework (ENS).</p> <p>Biannual review of the national list of entities becomes annual</p>
--	--

- The differentiation between essential and important entities should also provide greater legal certainty. These categories are subject to obligations without considering their scope of application or the risk intrinsic to each business. Based on the above, the terminology and criteria for differentiating between “essential” and “important” entities should be improved, as well as the obligations that would apply to those entities (for example, digital service providers) that provide various services in the EU and that may be in the scope of both Annex I and Annex II.
- Clarify the territorial scope of the "manufacturing" category in Annex II, particularly if it is carried out outside the EU, if the intention is to include manufacturing processes that exceed national or European scope in the regulation.
- Align the definition of cloud computing services to the definition established in other European regulations and standards.

**Inclusion of hardware and software providers in the scope of the proposal.**

The proposed Directive does not propose a comprehensive framework on the security of products and services offered by SW and HW suppliers, unloading the weight of regulation on the entities that provide essential services, despite highlighting the importance of security of the supply chain.

The Directive sets out to address this challenge from an aggregate of partial solutions: (1) in client-supplier contracts, (2) with the application of certification schemes, to date voluntary in the private sector and in the definition phase and (3 ) by including in Annex II of the Directive (important entities) a small part of these agents (manufacturers of electronic equipment and computers). However, Annex II does not make any reference to software providers, when in reality the most frequent and high-impact security threats are related to software components (consider also the growing relevance of SW in the process of virtualization of IT systems and in electronic communications architectures). In this sense, it will be necessary to deepen and specify what regulatory measures it would be necessary to establish to mitigate cybersecurity threats originated by HW and SW components, as well as the elements of co-responsibility of the agents involved in the process (for example due to the incorrect software configuration or bug patching by the manager)

There is a risk that these three types of measures are a mosaic of partial solutions. Therefore, it is proposed to adopt a more agile and effective approach based on establishing the scope of direct responsibilities to be determined for SW and HW providers within the framework of the Directive.

	<p>As in other sectors, such as automotive or aeronautics, where the equipment manufacturer is responsible for serious failures caused by its components, it would be expected that SW and HW suppliers and service providers have direct legal responsibility for security failures generated by its equipment and services, and not only through the contractual relationship.</p> <p>Therefore, HW and SW providers should be subject to minimum regulatory requirements equivalent to essential service providers defined in a horizontal regulation (as indicated in the EU Cybersecurity Strategy) in order to offer an improvement in cybersecurity and end-to-end resilience of the elements involved in the delivery of a given essential service. The different mechanisms that allow offering these minimum guarantees in terms of cybersecurity and resilience remain to be specified.</p>
--	--

### **Clarify the public administration entities that are in the scope of NIS 2**

The article 2 of the proposal includes explicitly public administration entities: *“Article 2. Scope...However, regardless of their size, referred to in Annexes I and II, this Directive also applies to entities where:...(b) the entity is a public administration entity as defined in point 23 of Article 4;”*.

Art. 2.2 refers to a list of entities to be submitted to the Commission: *“Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.”*

On the other hand, annex I points to the public administration entities that would be included: *“ANNEX I ESSENTIAL ENTITIES: SECTORS, SUBSECTORS AND TYPES OF ENTITIES... 9. Public administration ... - Public administration entities of central governments - Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 (27) - Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003”*.

The definition of point 23 of Article 4 is based on a set of cumulative criteria, not referred to Annexes I and II. From this definition together with art. 2.1 and 2.2, it is not possible to have a clear picture of the public administration entities in the scope of the proposal.

**The Commission should clearly determine the public administration entities included in the scope of the proposal.** In principle, it seems that entities of central governments and regional administrations are included, but it is unclear the situation of entities of local and provincial level administrations.

At least the following provisions shall affect to entities of public sector in the scope of the Directive:

- Article 15 Report on the state of cybersecurity in the Union
- Article 16 Peer reviews

- Article 18. Cybersecurity risk management measures, part 2 *“The measures referred to in paragraph 1 shall include at least the following:...”,* part 5: *“The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2.”,* part 6: *“The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2...”*
- Article 20. Reporting obligations
- Article 21. Use of European cybersecurity certification schemes
- CHAPTER VI Supervision and enforcement

**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.

We acknowledge the efforts carried out in the proposal for amending Regulation (EU) No 910/2014 to improve the approach on security requirements and notification of incidents and to give more coherence between the NIS2 and eIDAS frameworks. The proposal introduces cooperation mechanisms between NIS2 and eIDAS authorities, and develops art. 24 in order to clarify that NIS2 security obligations are complementary and do not replace eIDAS security obligations for qualified trust service providers (QTSP). However, some important issues in the NIS2 proposal still remain:

**- We are of the opinion that modifying a Regulation by means of a Directive is not the ideal approach and still poses doubts about a potential decrease in the level of harmonization.** Moreover, although NIS2 proposal now foresees that deletion of art. 19 entries into force after the end of the transposition deadline, there are serious doubts about how the “gaps” in the transitional

periods. At this moment, we understand that eIDAS proposal needs to be read assuming that by the time of its adoption art.19 will be deleted by the NIS2 Directive, but this might be not the case. More clarification would be needed about these aspects. Also, it has to be taken into account that each Member State shall transpose NIS2 Directive at different points in time, thus creating many uncertainties regarding the application of eIDAS Regulation during the period of transposition. **It would be preferable to perform all the adjustments needed in the eIDAS Regulation within its own revision procedure, not in the NIS2 Directive context.** Instead of deleting art. 19, one idea to be explored could be modifying art. 19 in the eIDAS review in order to take on board the NIS2 complementary requirements needed to achieve a high level of security.

- We consider that the proposed cooperation mechanisms between NIS2 and eIDAS authorities are interesting, but at this stage it is not possible to have a clear view on how they would be implemented in practice. It is also worth mentioning that the proposal seems to be oriented towards a model where it is preferable that NIS2 and eIDAS competencies rely on the same authority. In cases where they are different authorities, we believe that the supervision will be extremely complex and difficult to handle in practice. The proposal also creates fragmentation in the supervision model, which is notably in contradiction with the adoption of implementing acts of art. 17 and 18 in eIDAS amendment proposal, aimed to increase harmonisation regarding tasks and cooperation procedures for Supervisory Bodies. It also implies an unnecessary overload for companies, as they would have to comply with two different frameworks related to security and report to two different authorities.

- It is also important to note that **Art. 24 of eIDAS Regulation only covers qualified providers**, therefore the problem related to the differences of scopes in eIDAS and NIS2 security requirements is not addressed for the non-Q providers. Furthermore, non-Q security requirements would be supervised by NIS2 authority and the rest of the obligations by the eIDAS authority, without any cooperation mechanism put in place for this case.

- **The important problems of including non-qualified trust service providers in the group of essential entities have not been addressed.** This implies that the NIS2 authority will supervise ex-ante the security obligations of non-Q TSPs, which may have an important impact for these companies and also for the authority. On the other hand, the eIDAS authority supervises this companies ex-post. This scenario is inconsistent and difficult to manage, even if the MS designated the same authority for NIS2 and eIDAS. We strongly oppose to the designation of non-Q providers as essential entities.

As stated above, there are open questions and serious doubts arise in relation to the role and cooperation mechanisms between NIS2 and eIDAS authorities, the notification of incidents procedures and the supervision of nonQ trust services providers. We consider that this compromise proposal has been introduced at a very late stage and without enough analysis and exchange of views and **we have serious doubts that it could lead to good results when implemented in practice.**

For all the reasons above, **we consider that the compromise proposal does not cover the main concerns raised in relation of Article 39 of NIS2 proposal** and it is not feasible to address those concerns by just including some clarifications in the text of NIS2 proposal. Therefore, in line with our contribution (amendment 5) **our position is that the supervision of security must remain in eIDAS framework. Trust services must be eliminated as a subsector of essential entities, in application of the lex specialis principle.**

**Member States need to have room to apply the provisions of article 2.2 (and those from implementing acts foreseen in 2.5 and 2.6) according to their national security frameworks (in Spain, “Esquema Nacional de Seguridad” - ENS)**

The National Security Framework in Spain (ENS) applies to the whole public sector (about 30.000 entities). The application of the ENS would help them to swiftly comply with the proposal, in particular with *CHAPTER IV Cybersecurity risk management and reporting obligations - SECTION I Cybersecurity risk management and reporting*, because it provides a common approach of basic principles, minimum requirements, security measures and procedures for auditing and conformity assessment by means of accreditation ISO/IEC 17065 standard by the National Accreditation Body (ENAC) of certification entities. The ENS not only applies to the public sector, but also to private entities cooperating with public sector entities in the provision of public services or personal data processing.

**More clarification is needed about the relation of the proposal with tools as the national security frameworks that Member States may already have in place, as is the case of the Spanish ENS**, in particular articles 15, 16, 18, 20 y 21. In particular, an important question is **if Member States will have room in the application of article 2.2 at a national level (and those from implementing acts foreseen in 2.5 and 2.6) according to their national security frameworks.**

The public administration entities included in the scope of the proposal (that also need to be further clarified by the Commission) constitutes only a subset of the whole public sector, therefore it is very important not to create duplicities or different models of security measures.

<b>ANNEXES</b>	This extension of the NIS Directive goes beyond the approach of basing critical sectors on critical infrastructure. The approach should be built based on the competent ministerial authorities.
	<p>The NIS 2 project suffers from <b>a lack of clarity that could impact on the legal security of the obligated subjects</b>, which it divides, on the one hand, into “essential entities” and, on the other, into “important entities” (see annexes I and II).</p> <p>If this is added to the fact that in the framework of the future CER Directive (which will replace the current CIP Directive) there is the figure of “critical entities”, which are those that provide essential services in the “physical” field, or not cybernetics, all of this can cause significant confusion for those subjects bound by both standards (which substantially coincide) and who could become subject to double regulations by different authorities. In Spain, although much progress still needs to be made, this problem is today largely solved with the alignment between PIC and NIS, and the figure of the Secretary of State for Security of the Ministry of the Interior as the authority of both systems, through of the CNPIC.</p> <p><b><u>The transposition of the future Directives (NIS 2 and CER) should not lead to the destruction of the existing system, but to improve it.</u></b></p>

## Article 17 Governance

1. Member States shall **ensure** that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.

***Comment: How will Member States ensure? It is suggested that for this "watch over" task, a brief report could be available as the process has been followed and the pertinent actions have been carried out to an analysis of risks, measures, etc.***

## Articles 27 to 22

<b>Art. 18</b> <b>Cybersecurity risk management measures</b>	<p>The establishment of specific criteria is valued positively.</p> <p>The establishment of obligations to ensure that the supervised entities implement the security measures in the shortest possible time without compliance deviations will mean a significant increase in the supervisory effort by the Supervisory Bodies.</p> <p>The "risk-based supervision" and "prioritization" proposed by the Commission are not a solution. A comparative diagnosis of risks among thousands of entities would be a monumental task. The closest process would be the designation of critical infrastructures based on the possible impact. For any finer-grained diagnosis it would be necessary to analyze ex ante how well each entity is protected. In the end, such "risk-based monitoring", even after immense diagnostic work, still would leave a lot of work to do. There are many entities with a great cyber risk. That is, assuming cybersecurity risk could be estimated reliably. It cannot. In practice, a "black swan" can appear from where you least expect it. And, if the Supervisory Body did not supervise the "black swan" entity, the blame will be on the Supervisory Body for misjudging its "risk-based supervision".</p> <p><b>18.1</b></p> <p>This section should be further specified.</p> <p>It is recommended the development of a set of common measures for all Members and that some provisions be articulated that allow assessing the application by national authorities of these provisions.</p> <p>A reference framework of security measures to be applied should be included. This has been done in Spain in the transposition of the previous NIS directive.</p>
---	--

Spain could propose the Spanish National Security Framework adapted as a possible model to be used by the rest of the countries.

## **18.2**

The measures indicated in paragraph 18.2 of Article 18 of the proposed revision of the NIS Directive broadly follow the spirit and letter of Article 2 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

The Supervisory Bodies' experience with the aforementioned Article 2 has been negative. It outlines broadly the elements of ICT Security standards, but it is too undefined to enforce even the smallest level of compliance with any ICT standard. This explicitly harmed supervision efforts, giving supervised entities a way out as long as they included the listed elements, as unsatisfactory as they may have been. It also created a de facto legal heterogeneity, as every MS's Supervisory Body interpreted Article 2 differently.

We therefore strongly request that in paragraphs 18.5 and 18.6, where it says that "The Commission may adopt implementing acts" this is substituted by "The Commission SHALL adopt implementing acts". And that an explicit deadline for these implementing acts is included.

It is also recommended that this section be enriched with the provisions of Royal decree law 12/2018. In RD Development of RDL 12/2018, the following are listed as minimum measures:

- a) Risk analysis and management.
- b) Risk management of third parties or suppliers
- c) Catalog of security, organizational, technological and physical measures.
- d) Management and professionalism of personnel.
- e) Acquisition of security products or services.
- f) Incident detection and management.
- g) Recovery plans and assurance of the continuity of operations

<p>Article 19</p> <p><b>EU coordinated risk assessments of critical supply chains</b></p>	<p>The NIS2 proposal indicates that entities are responsible for the companies that participate in their supply chains; Article 18 (3) obliges entities to take into account the particular vulnerabilities of each provider. This obligation is not realistic given that many essential and important entities have little or no control capacity not only over large global IT companies but also over companies with which they usually operate, whether in a direct relationship or not, depending on their position in Supply Chain. It is essential that the NIS2 proposal provides guidance in order to put into practice the obligation established in article 18. In this sense, it is proposed that those companies that manage a significant number of clients are subject to certifications based on international standards such as National Security Framework of Spain or ISO 27001 previously mentioned or others (SOC, NIST, C5, etc.) carried out by independent auditors that guarantee that risk management and risk mitigation are carried out on an ongoing basis along with initiatives and good practices.</p> <p>It is also proposed that the Commission take into consideration global industry-led initiatives in this area, such as the recommendations of the Charter of Confidence for Cybersecurity regarding basic security requirements in the digital supply chain or the promotion of risk management in the supply chain through external security assessments of suppliers, products and services (Art.18 (2d)). The basic requirements must be complemented with a security approach by design of products and services.</p>
---	--

<p><b>Article 20 Reporting obligations</b></p>	<p>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.</p> <p>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.</p> <p>The second characteristic is that these behaviors and facts must be public, knowable, ascertainable to the sanctioner. And proveable.</p> <p>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.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Article 20.2 states "2. Member States shall ensure that essential and important entities notify, without undue</li> </ul>
--	--

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 appropriate", 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 significant 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.

<p><b>Article 21</b></p>	<p>The proposed Directive, in addition to introducing new elements, must take into consideration the existence of existing national tools that have proven their effectiveness over the years in the field of cybersecurity. This is the case, in Spain, of the National Security Framework (ENS-NSF).</p> <p>The National Security Framework (ENS-NSF) is especially important because:</p> <ol style="list-style-type: none"> <li>1. It is a cybersecurity evaluation and certification scheme regulated by law, approved by the Spanish Parliament in 2010.</li> <li>2. It applies to the entire Spanish public sector (some 30,000 entities) and also applies to companies providing services to public entities.</li> <li>3. The number of evaluated and certified entities is several hundred.</li> <li>4. It is a scheme specifically aimed at ensuring the security of the provision of public services, with all the importance that this entails, with particular impact on Chapter IV Cybersecurity risk management and information obligations, as it provides a common approach to basic principles, minimum requirements, security measures and audit and conformity assessment procedures through the accreditation of certification bodies against the ISO/IEC 17065 standard by the National Accreditation Body (ENAC), as well as the monitoring of the status of entities within the scope of the ENS.</li> </ol> <p>All these reasons more than justify the need to respect this evaluation and certification scheme, allowing the permanence of the ENS-NSF and its coexistence with the other new schemes that may be implemented in the EU.</p> <p>The art. 21 (paragraph 2) should be modified to allow the coexistence of European and National frameworks like the ENS-NSF:</p> <p style="padding-left: 40px;">&lt;&lt;Article 21. Use of European cybersecurity certification schemes</p> <ol style="list-style-type: none"> <li>1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.</li> <li>2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The</li> </ol>
--------------------------	--

	<p>delegated acts shall be adopted in accordance with Article 36 <b><u>and may provide that the certifications referred to in paragraph 1 correspond to certifications regulated in the Member States, legally enabled, which provide at least the same degree of security as the European Cybersecurity certification.</u></b></p> <p>3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.&gt;&gt;</p> <p>Given that the entities of the public administrations in the scope of the proposal are a subset of the group of entities of the public administrations (and the Public Sector), it is considered very important that there are no scenarios of duplication of security measures &gt;&gt;</p>
<b>Article 22 Standardisation</b>	<p>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.</p>

## ARTICLES 28 TO 33

<b>Art. 29 Supervision and enforcement for essential entities</b>	<p>The <a href="#">Spanish National Security Framework</a> includes these obligations. Perhaps it is better to implement this type of national scheme and carry out security audits based on the set of measures established nationally. They should not be based on risk assessments due to their heterogeneity, which would lead to higher costs and different criteria in different Member States.</p> <p><u>Incidents sometimes affect several Member States. This article should mention explicitly that essential entities have an obligation to notify the national CSIRT of each affected country, answer the prompts and questions of the national CSIRT of each affected country about incidents and send updates of the information about the incidents to the national CSIRT of each affected country. Minimum SLA's could be developed in an implementing act. The SLA's should be different according to the level of criticality and impact of the incident.</u></p>
	<p>Deepen supply chain monitoring</p>

<p><b>Article 30</b></p> <p><b>Supervision and enforcement for important entities</b></p>	<p><u>Incidents sometimes affect several Member States. This article should mention explicitly that important entities have an obligation to notify the national CSIRT of each affected country, answer the prompts and questions of the national CSIRT of each affected country about incidents and send updates of the information about the incidents to the national CSIRT of each affected country. Minimum SLA's could be developed in an implementing act. The SLA's should be different according to the level of criticality and impact of the incident</u></p>
<p><b>Article 31</b></p> <p><b>General conditions for imposing administrative fines on essential and important entities</b></p>	<p>This article should explicitly mention that, although all Member States must comply with these requirements, they are free to impose further criteria.</p>

## SWEDEN

NIS2 art. 2, 17–22 and 28–33 – SE comments and initial drafting proposals

As announced by the Slovenian Presidency, MS are invited to send in comments and initial drafting proposals on Article 2 and Annexes, and Articles 17-22, 28-33 by Thursday, 24 June 2021, COB.

*Please note, that the following comments are not exhaustive and might be elaborated further. SE is still scrutinising the proposal as a whole.*

Art.	COM proposal	Presidency first compromise proposal	SE Change request	SE Initial drafting proposal
<b>Scope</b>				
<b>Art 2, para 1</b>	This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.28		SE does not see any added value with the size-cap rule as the main criteria to determine whether entities should be targeted by NIS. The criteria would have negative impact and consequences for many entities. The “one size fits all” threshold doesn’t consider the different size, structures, and markets of Member States. The current proposal does not consider the principle of proportionality in a sufficient way. For example, the current proposal would mean that some critical small enterprises could fall outside the scope of the NIS directive while others, such as independent retailers, would be included. The definition of the scope needs to be more contextual and Member	As we still need more time for national analysis we will not be giving a specific drafting proposal at this stage for this article.

			<p>States should be able to adjust threshold levels. In this way it would be easier to target relevant entities and meet the actual needs in the Member States. Some flexibility at the national level should therefore remain.</p> <p>Moreover, SE would like a clarification of what might be the added value in including Banking and Financial market infrastructures under the scope of NIS2 (see Annex I, Sector 3 and 4), now that these entities will be covered by DORA. The way we see it, the provisions on information sharing and cooperation between NIS-authorities and DORA-institutions can exist independently of the scope of the NIS2-directive. We therefore appreciate if this matter is further elaborated on and explained.</p>	
<b>Art 2, para 1</b>	<p>However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:</p> <p>(a) the services are provided by one of the following entities:</p> <p>(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;</p> <p>(ii) trust service providers referred to point 8 of Annex I;</p>		<p>SE considers that the inclusion of Sector 9. Public Administration raises concerns on issues such as subsidiarity and national security. SE considers that the sector public administration should be Member States sole responsibility and that it should be up to each Member State to decide if and in that case which entities should be targeted by the NIS.</p>	



<p>(iii) top-level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;</p> <p>(b) the entity is a public administration entity as defined in point 23 of Article 4;</p> <p>(c) the entity is the sole provider of a service in a Member State;</p> <p>(d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;</p> <p>(e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;</p> <p>(f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;</p> <p>(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council<sup>29</sup> [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity</p>			
---	--	--	--

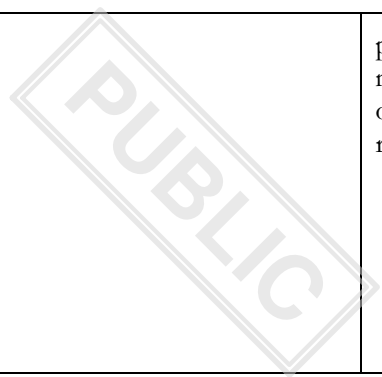
	<p>pursuant to Article 7 of that Directive.</p> <p>Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.</p>			
<b>Art 2, para 3</b>	<p>This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.</p>	<p>(...)</p> <p>This Directive is without prejudice to the <b>responsibility</b> competences of Member States <del>concerning the maintenance of</del> <b><u>regarding essential State functions concerning</u></b> public security, defence and national security <b><u>in accordance with</u></b> compliance with Union law.”)</p> <p>3.a This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.</p> <p>(...)</p>		<p>This Directive <b>does not</b></p> <p><b>(a)</b> affect the <b>sole</b> responsibility of Member States to <b>ensure safeguard</b> national security or their power to protect <del>their other</del> <b>essential state functions</b> security interests <del>[Alternatively: This Directive does not hinder any actions to ensure Member States national security or to protect their essential security interests].</del> In particular, <b>this Directive does not</b></p> <p><b>(i)</b> apply to entities with importance to Member States' defence or national security, <del>including law enforcement and judiciary.</del></p> <p><b>(ii)</b> <del>Furthermore, the Directive</del> oblige <b>Member</b> States or entities to supply information where such a supply of information would be contrary to national security <b>or defence interests,</b></p> <p><b>(iii)</b> apply to those activities of</p>



				<p>entities, which fall outside the scope of Union law and in any event all activities concerning national security and defence, regardless of who is carrying out those activities whether it is a public entity or a private entity acting at the request of a public entity.</p> <p>(b) apply in the area of public security and the judiciary. In particular, this Directive does not</p> <ul style="list-style-type: none"><li>(i) apply to entities with importance to Member States' judiciary and public security, including public administration entities to any extent concerned with law enforcement,</li><li>(ii) oblige Member States or entities to supply information where such a supply of information would be contrary to public security,</li></ul>
<b>Art 2, para 5</b>	Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this	<b>5a.</b> To the extent that is <b>strictly necessary and proportionate for the purposes of ensuring the security of network and information systems of essential and important entities, competent authorities, SPOCs and CSIRTs may process special categories of personal data referred to in Article 9 (1) of Regulation (EU) 2016/679</b> subject		Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities <b>according to this Directive</b> only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to

	Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.	<b>to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.</b>		the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.
<b>Governance</b>				
<b>Art 17, para 1</b>	Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.		Management bodies should be assigned a greater responsibility regarding cybersecurity. It should be up to the Member States to decide which measures are necessary and how they should be applied.  Further, there are some ambiguities in this article. The purport of “to be accountable for the non-compliance” is unclear, as well as how this would be managed in practice.	Member States <del>shall</del> <b>should</b> ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, <del>supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.</del>
<b>Art 17, para 2</b>	Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations		It is unclear what specific training on regular basis means. Could it be clarified?	

	of the entity.			
<b>Cybersecurity risk management measures</b>				
<b>Art 18, para 6</b>	The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.		The Member States should be involved in the process of specifying which categories of essential entities shall be targeted by such requirements. It is also proper that such decisions require Member States' approval. Due to this SE wants the delegated acts to be excluded from the Directive and if appropriate that the implementing acts should be used.	The Commission is empowered to adopt <del>delegated</del> <b>implementing</b> acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.
<b>Reporting obligations</b>				
<b>Art 20, para 3</b>	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.		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".	
<b>Art 20, para 9</b>	The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses		SE considers that this frequency is not motivated with regards to the administrative burden that it would impose. The need for this reporting frequency is not justified.	The single point of contact shall submit to ENISA on an <del>monthly</del> <b>annual</b> basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the



	notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.			provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.
Use of European cybersecurity certification schemes				
<b>Art 21, para 2</b>	The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required <b>to use certain certified ICT products, ICT services and ICT processes</b> or obtain a certificate <del>and</del> under <del>which</del> specific European cybersecurity certification schemes <b>adopted pursuant to Article 49 of Regulation (EU) 2019/881.</b> <del>pursuant to paragraph 1</del> The delegated acts shall be adopted in accordance with Article 36.		The Commission shall be empowered to adopt <del>delegated</del> <b>implementing</b> acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The <del>delegated</del> <b>implementing</b> acts shall be adopted in accordance with Article 36.