Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 07 April 2021

WK 4633/2021 INIT

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI

WORKING PAPER

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 - Comments and questions by BE, CZ, DK, FI, HU, IE, IT, LV, LT, LU, SI, ES and SE on Articles 24-34

Delegations will find in Annex comments by BE, CZ, DK, FI, HU, IE, IT, LV, LT, LU, SI, ES and SE on Articles 24 - 34.

TABLE OF CONTENT

BELGIUM

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

Art. 24 & Recital 63 – Jurisdiction & Territoriality

- The title of article 24 (*Jurisdiction and territoriality*) is confusing: it seems at first to cover all sectors, while it only deals with digital infrastructures and digital service providers.
  Why is the jurisdiction for other sectors not specified here (and only mentioned in recital 63)?

Recital (63): [Essential & important entities -except those from art. 24- including those providing f.e. cross-border services will] *fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of those Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions*.

- Hence, such entities might have to comply with a collection of reporting obligations, supervision rules & sanctions that can be different in each Member State where the entity provides services.
- The rationale provided to assign one single jurisdiction to the entities from art. 24(1) seems to be that they *provide services across borders to a particularly high extent* (cf. rationale given to appoint one single jurisdiction to the entities from art. 24(1) in the *Detailed explanation* on page 11 of the proposal).
  Albeit, this argument also applies to a multitude of other entities that provide cross-border services or services in multiple MS. Take as an example a train company delivering cross-border freight transport, i.e. activities in multiple member states.

Art. 24– Jurisdiction (digital service providers): quid other sectors?

(1) *shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union*

- **Why is this only foreseen for the specific (digital services) entities and not for all entities?**
- How can the ***main establishment*** (and associated jurisdiction) be determined for the application of article 24?
  In case this is determined by (national) commercial law, we are afraid that the possible options (place of the statutory/registered office versus place of the centre of decision) will create confusion in case of activities in multiple member states.
- Which jurisdiction will f.e. apply to an essential entity founded in MS A (though no activities in MS A), with activities in MS B and also activities in MS C?

(2) *where the decisions related to the cybersecurity risk management measures are taken […] or with the highest number of employees in the Union*

- Will it be the meeting place of the board of directors who ratifies the decisions [related to cybersecurity risk management] or rather the places where the operational people who make day-to-day decisions are located?
  - If the Chief Information Security Officer often works in two establishments in different member states (or indeed works from home) or two establishments would have an equal number of employees, would the entity than be free to choose which one of these is the main establishment?

- Given the registration obligation in art. 25, is it correct that the provisions in this article mostly steer the hand of the entity in declaring its main establishment? Or is there still burden on the Member States to find out whether the entity's declaration is correct.
- Wouldn't it be preferable, for reason of legal certainty, to have a more stable criterium than the MS with the highest number of employees in case the decision is not taken in any MS, at least for such important thing as the jurisdiction.
  Isn't the *place of the statutory/registered office* a more stable criterium providing for far more legal certainty anyway?

(3) *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.*

- What if an entity is non-compliant because of non-compliance of his supplier but has no means to enforce the measures to his supplier?
- How will the actions of the Member States be aligned if these measures are to be taken?
- A deadline could usefully be set for the appointment of a representative (e.g. X months after the entry into force of the Directive or X months after the first activity on the European territory for new activities that are being created).
- Furthermore, the penalty for failure to appoint a representative should not lead to a situation which could be chaotic as regards the lead authority in the event of competing actions by several MS.

(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.*

- Can the representative be seized only as the company's representative or will it be necessary to seize both (the company and its representative) or will it be necessary to seize all the related companies in order to be sure of being able to designate the entity which will ultimately be considered as the "main establishment"?
  Doesn't this risk creating legal uncertainty?

Art. 25– Registry for important & essential 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]:*

- Can the Commission clarify what is the objective, the finality and added value of this register?
- Wouldn't it be more logic to have ENISA as a consolidator of information that entities have submitted to (their) competent authority (sectoral authority or national single point of contact), instead of the other way around (as proposed in art. 25)?
  In our opinion this is even required, in order
  - to avoid the existence of different lists (ENISA versus SPoCs);
  - to avoid dissemination of Points of Contact for the companies;
  - to avoid separating the management (ENISA) from the enforcement (MS) role.

- How can entities submit information to ENISA before the directive has been/has to be transposed to national law?
- Will this register be published?
  - If not, who will have access to it? The MS for all stakeholders?
  - Is this public information, or only for competent authorities?

    - **What would be the impact on EPCIP legislation for which some MS (including BE) have decided not to publish the criteria and identity?**
    - Would other Member States be able to consult the (entire) Registry (or only what has been *forwarded by ENISA, cf. art. 25(3))*? (If an entity offers services in their country, a MS should be able to know which MS has jurisdiction?)
- There is no mechanism for entities of art 2.1 to report their « self-identification » as essential entity. Does COM provide a (similar) framework for identification notification (or registration mechanism) to the Member States? **If not, how does COM see the information flow for the MSs if they are to perform their supervision tasks concerning the entities in art. 2.1?**

(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.*

- Art. 25 seems to cover only the situation at the entry into force of the Directive. What will happen to new entities that are created in subsequent years or that start the indicated activities only after this date? Will they have to notify within three months on the basis of §2? If so, this should be clarified in the provisions.

(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*

- Will ENISA make use of the information received for other purposes than for forwarding it to the national authorities?
- Will ENISA also *publish* this information (to *all* single points of contact), so that it is accessible not only to the single points of contact *depending on the indicated location of each entity's main establishment* (but also to other MS' single point of contacts)?

(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.*

- Shouldn't (4) also make reference to (2), including the case of new such entities?
- What exactly will be the responsibility of Member States in this respect? Will they have to inform the Commission/ENISA in case of non-compliance? If so, through which channel(s)?

Art. 26– CS information-sharing arrangements

(1): *essential and important entities may exchange relevant cybersecurity information among themselves* (and (2): *the exchange of information takes place within trusted communities of essential and important entities*)

- Does this wording not exclude national or sectoral CSIRT's to be part of such exchanges of info? Would it not be highly relevant for them to also have awareness of such information (especially given their obligations under art. 10(2))?
- Would it not also be unfair and expensive for Member States to have to set up such exchanges, but not be allowed participation?
- Is the exchange organized between the essential entities without the Competent Authorities (CA) present or informed about the content of the shared information?
- What if the CA's with supervisory competence are also public administration entities? What is the view of COM on the relation between these responsibilities?
- Will the exchange of information also include security measures of art. 18? If yes, how can this be ensured?

(2): […] *trusted communities of essential and important entities*[…]

- Given the enormous enlargement of the scope, the community of essential and important entities could become very big. **How trusted and useful could such a group still be if it is so large?** (The idea of a trusted community being to allow sharing of information that should not be shared with anyone, for reasons of confidentiality).
- Does the Commission/ENISA envisage to develop/provide tools to support such *trusted communities?* This could be cost-efficient and cater for compatibility amongst MS, and could even promote f.e. sectoral inter-MS communities (hospitals as an example).
- Does the Commission/ENISA envisage to develop information sharing protocols to take into consideration sharing limitations such as TLP-codes, national law confidentiality stipulations (e.g. specific constraints applying to information that is part of a police or judicial investigation), storage requirements (encryption requirement f.e.)?
  We refer to initiatives such as the "Info Exchange Protocol". Such protocols would not only be useful for the information sharing of art. 26, but also for inter-CSIRT sharing.
- What is meant by "**trusted entities**"? Trust is not something that can be "forced" but it must be generated gradually. If the entities are identified as essential or important, they are directly concerned by this exchange. How is this aspect of trust envisaged by COM in concrete terms?

(3): *Member States shall set out rules specifying the procedure, operational elements* […]

- What is the concrete role expected of the MS?
  Simply providing a platform?
  Monitoring, information management, encouraging the creation of circles of trust (through binding legal instruments?), ...?

(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.*

- How is participation or withdrawal decided?
- Does the competent authority or the essential/important entity decide on this?
- Is participation mandatory or voluntary for the essential/important entities?
- According to §4, membership of the platform seems to be optional for essential and important entities since they can opt out freely: is this the case?
  - What if an entity concerned by an incident is not connected to this platform?
    - Does the sectoral authority itself have to be connected and then transmit the information through another channel?
    - Or are sectoral authorities excluded from these platforms? If so, how can it be ensured that the information exchanged will not harm national interests (national secrets) and that the necessary information actually reaches the entities concerned?
- What is the role of the competent authority following a notification via such community arrangement?

(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.

- Does this also have a link with cert.eu?

Art. 27– Voluntary notification

- If a non-essential or non-major entity decides to notify an incident when it is not obliged to do so, it seems to us that it generally will be an important notification that can prevent harm to third parties. In the event that a Member State chooses not to prioritise such voluntary notifications, we question the responsibility of the Member State to the notifiers and to third parties.
- Is anyone allowed to report (anything) *voluntary*? How can we ensure that the input provided is of good quality? Will entities providing voluntary notifications be given access to any (further or similar) information?

Art. 28-34– Supervision & Enforcement -Financial sector

- NIS2 should explicitly state that these provisions do not apply, on the basis of the lex specialis principle, to the supervision of financial entities that are in scope of DORA.
- Similarly, 34.1. (b): *a competent authority may request another competent authority to take the supervisory …measures…* and (c): *a competent authority shall,…, provide the other competent authority with assistance…*"
    - given the independency of Central banks and the confidentiality of prudential control information, it should be explicitly mentioned that these provisions (Art 34) do not apply to the financial sector.
    - "*A competent authority to which a request for assistance is addressed may not refuse that request unless…*": this formulation is too strong and should not apply to the financial sector.

Art. 28 - Supervision & Enforcement -General aspects

28 (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.*

- What should we understand by ***monitor and take the measures necessary for compliance***? How should we evaluate the application of this article?

(2): *Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches*
and 32: *Infringements entailing a personal data breach*

- Can the Commission clarify what is meant with this provision, as it is up to the essential and important entities to do the necessary reporting to the relevant data protection authorities, in accordance with GDPR.
- If these provisions are maintained, they should be made mutually applicable, in the sense that data protection authorities must inform NIS2 authorities when they have indications that the infringement by an essential or important entity of its GDPR obligations also entails a breach of its obligations under NIS2.
- What will happen in the case of data breaches *other than personal* data (technical, financial, etc.)?

Art. 29– Supervision & Enforcement (essential entities)

General remarques:

- How is defined which Member State has jurisdiction over an essential and important entity not mentioned in article 24. 1? An entity with cross-border activity could be sanctioned in two MS for the same infraction (ne bis in idem).
- How is defined which Member State has jurisdiction over the supplier?

- Which set of security measures and which supervisory regime of which Member State will apply to the entity?
- Which set of security measures and which supervisory regime of which Member State will apply to the supplier?

(2) a: [..] *on-site inspections* [..]

- How is jurisdiction decided here? If an entity offers services in MS X, but it has a site in MS Y, does the competent authority of MS X have jurisdiction to request on-site inspection in MS Y (in collaboration with MS Y of course)?

(2) d: *security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;*

- How are ***security scans*** to be understood?

(2) 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.*

- What does "qualified auditor" mean?

(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****.*

- In the context of an inspection, it is not always easy to determine in advance all the information that will be requested. Indeed, this may also depend on what is discovered on the spot. The phrasing sounds as if any information that was not requested initially cannot be requested in the course of the inspection.
  Could this part of the sentence therefore not be inspired by other provisions (e.g. economic inspections) or make a reference to the fact that all necessary information must be transmitted to the authority concerned?

(4) i: *make a public statement which identifies the legal and natural person(s) responsible for the infringement* (idem art. 30(4)h)

- Would this provision not harm trust between competent authority and essential entity? Is such 'naming and shaming' a proportionate and useful instrument?
- Would a public statement about infringement not publicly expose an essential entity as a potentially easy target for criminals – as we would be explicitly stating that the entity is not sufficiently protected? Would competent authorities not be putting the entity – and thereby its essential services to society – at unnecessary risk?

(5) a: *Member States shall ensure that the competent authorities have the power to 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.*

- What's the relation of such suspensions with the national basic principles that should guarantee the continuity of public service in the Member States?
- (How) Can the term "Authorisation bodies" be mapped to standard ISO terminology such as Certification bodies or assessment bodies (audit firms) and Accreditation bodies (national supervisors, like BELAC/RVA/COFRAC/DAKKS, …)?
- What is the consequence of the suspension of a certification or authorization? Can the competent authorities suspend a service that is essential for society?

(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.*

- How is the constitutional principle of separation of powers guaranteed for the application of such temporary ban on responsibilities at the level of the managing director or legal representative of the essential entity or other natural person held liable?

(6): [..] *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.*

- Managers (natural persons) and entities (legal persons) should be considered as responsible. However, a representative, is not "responsible" but "representative". As he does not have the power to really influence the strategic decisions of the company, his personal liability should not be engaged. On the other hand, seizing the representative should be sufficient to seize the entity he represents as well. As regards people who take decisions on behalf of the company, there should be a reference to strategic decisions (outside the usual work) in order to exclude f.e. civil engineers and computer scientists who take daily decisions in their usual work but who never had in mind to engage their personal responsibility.

… those natural persons may be held liable for breach of their duties to ensure compliance…

- What exactly is meant by liable? What actions could be taken against them?
- Does this mean that there is a possibility to impose criminal sanctions on that natural person or does it refer to § 5, point (b) of article 29 of NIS.2 or does this mean that competent authorities can impose sanctions on a company who will then internally blame it on their representative and take the necessary internal actions? In any case, there needs to be clarification on this point.
- Could this provision not harm trust between a CEO and their CISO, which is crucial for security?
- Does this only apply to top management, or also to CISO-level?

(7): *Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5…*

- Why not also pursuant paragraph 6?
- Does the seriousness of the offences listed under (a) fall within the scope of cybercrime as referred to in the EU Operating Regulation, in particular Article 83?

Art. 30 – Supervision & Enforcement (important entities)

- The proposed definition of essential and important entities would have a huge impact on the MS and the entities concerned. As an example, in the Energy sector, instead of supervising the main entities, several hundred entities would be targeted tomorrow.
- In order to avoid this, to mitigate the impact and to keep a proportional aspect, would it not be possible to leave some room for manoeuvre for the MS to determine whether these entities should really be considered as essential entities or whether at least some, or certain sub-categories of them could not be reclassified as important entities instead?

Art. 31 – Administrative fines

(4): *… administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover […] which ever is higher.*

- How should we interprete this minimum value for the maximum fine? What is the role of national legislator in this regard?
- Why this amount? Is it not disproportionate, for example as 10 million € could be the total annual turnover of some of the (Medium sized) organizations in the original scope?

(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.*

- How should the term ***periodic penalty payments*** *be* understood? Is it *une astreinte (FR)/ dwangsom (NL) ?*

Art. 32 – Personal data breach

(1): *Where the competent authorities have indications [..] they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within a reasonable period of time*

- How should ***within a reasonable period of time*** be understood?

(3): *Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority…*

- Could the Commission clarify (provide an example) how a supervisory GDPR authority could be established in a different Member State than the competent authority for NIS.2?
- Furthermore, how would the competent authority be able to know the GDPR attribution rules and be able to determine with certainty which supervisory authority in which MS it should notify? This is not within the authority's competence.

Art. 33 – Penalties

- Could two or more Member States impose fines (art. 31) and penalties (art. 33) on the same entity for the same non-compliance if it has effect in more than one Member state? These fines could thus be different (and cumulative)?

Art. 34 – Mutual Assistance

(1): *Where an essential or important entity is providing services in more than one Member State*

- Entities are in or out of the scope of the directive based on the type of entity that they are or to what sector they belong, as established in the Annexes; so not necessarily on the type of services they provide. Jurisdiction, however, seems (it is not defined) to be decided by the services that these operators deliver. Are there not many possible gaps in jurisdiction here?
- Take an essential entity founded in MS A (though no activities in MS A), with activities (including main establishment) in MS B and also activities in MS C? Which of these member states will be obliged to deliver mutual assistance to each other?
- Certain manufacturers are in scope in Annex I & II: What is the basis of the scope and the jurisdiction? Does it
    - a) only concern manufacturers with establishments or factories in Europe?
      If so, does manufacturing that is done outside the EU then remain out of scope? Or do they also have to indicate a representative establishment within the EU, as is required for certain digital infrastructure entities?
        - Would this not give EU entities a disadvantage, as they would have to comply with security measures, whereas their often already cheaper non-EU counterparts would not?

- Or b) only/also those who are selling their manufacturings on a European market from outside the EU?

  If so, (and in case they sell to many MS) would not all those MS have jurisdiction over such entities? Who should coordinate the enforcement then?

  - How would on-site inspection then be enforced if the production site is outside the EU?
  - How will cooperation and assistance with those States take place?

(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.*

- Which mechanisms will be put in place to implement those *joint supervisory actions (art. 34 (2))?*
- Would the objective of such joint actions be to communicate and apply one single common and shared coherent set of rules on supervision & cybersecurity obligations?
  - If yes, how will such set be defined?
  - If no, would it be possible to designate one single supervising national authority (assisted by other Member States' authorities) and the associated jurisdiction, in order to increase transparency for both the entity and the supervising authorities?

CZECH REPUBLIC

ART. 24

Why the provision regarding the general jurisdiction over the essential and important entities other than those referred in Art. 24 was not included in the normative part of the NIS 2? That provision has paramount practical implications for supervision and enforcement of the Directive.

NIS 2 does not contain any provision concerning situations when one or more Member States would like to identify any of the entities referred to in Art. 24 on the basis of the criteria in Art. 2 paragraph 2, letters c)-f). The entity so identified could have its main establishment in a Member State other than that in which it has been identified. How would these situations be dealt with?

ART. 25

What was the basis for the assumption that one year provided for self-notification to ENISA would be needed? Similarly, what led the Commission to assume that three months provided for the notification of changes to contact details of entities enlisted in the ENISA registry under Art. 25 would be sufficient to serve the registry-related regulatory purposes?

ART. 26

The article is related to the national information sharing only. Would not it be beneficial to facilitate information sharing between entities from different Member States as well? Should not be cross-border information sharing considerations covered by this Article?

ART. 29 and 30

It would be welcomed if the Commission provided an explanation of the following terms used in the chapter on supervision and enforcement, including an explanation of differences between them:

On-site inspection

Off-site supervision

Random checks

Regular audits

Targeted security audits

Security scans

For the sake of clarity and facilitation of a harmonized implementation of the Directive, an introduction of corresponding definitions in Art. 4 or an explanatory recital should be considered.

ART. 30

How could the non-compliance with NIS 2 be demonstrated so that the Member States could obtain evidence or signs about it? **What kind of evidence or indications would allow the Member States to exercise their supervisory tasks?** What would be the likely use cases of (alleged) NIS 2 non-compliance in this context? Simply put, when and how could the supervisory powers be triggered?

DENMARK

(general remark)

- neighbouring countries cooperation in the NIS Cooperation Group and CSIRT-Network: Cross-border dependencies and incidents may include sectors of systems in neighbouring countries. In line with long-standing close collaboration the EEA-countries, provisions might be made for these countries to be invited to take part in the cooperation in the NIS Cooperation Group and CSIRT-Network as observers, provided that they establish a Single Point of Contact.

Article 24 (Jurisdiction and territoriality):

- decisional powers moved to another MS: (The provision concerning jurisdiction is much clearer defined in NIS2 than in the current NISD. Main establishment in the Union is the MS where decisions related to the cybersecurity risk management measures are taken. However, decisional powers related to cybersecurity may easily be moved to another MS). What happens if decisional powers related to cybersecurity, are moved to another MS during an investigation of complying with the directive, or during an enforcement procedure? Would the competent authority, where the entity originally had its main establishment, still be able to finalize the investigation/the enforcement procedure, or is it the competent authority in the MS where the main establishment has been moved to that has to take over the case?

Article 25 (Registry for essential and important entities):

It is positive that NIS2 includes a Registry for essential and important entities.
However, the proposed Registry does not contain information about the type of entity, e.g. whether an entity is a cloud computing service provider, a provider of online marketplace or both.

- type of entity: Is there a reason for why the registry does not contain information about the type of entity?
- differences: If there is a difference between the main establishment as defined in article 24 (2), and the information contained in the Registry, would it then be article 24 (2) that determines who the competent authority is?
- registry not updated: If a competent authority starts a supervision of an entity, based on the information in the Registry, would the authority then have to terminate the supervision, if the information in the Registry is not updated?

Article 26 (Cybersecurity information-sharing arrangements):

- (2) "information sharing arrangements": Could the Commission possibly elaborate on what is meant by "the MS shall ensure information sharing arrangements", and which tasks that the MS has to undertake to fulfill this responsibility?
- (3) information sharing if entities created their own network: If the MS has to set out the rules for information sharing, how does this provision affect a situation in which the entities themselves have created their own networks for information sharing? Would the competent authorities then have to impose themselves on the network?

Article 28 (General aspects concerning supervision and enforcement):

- (2) "addressing incidents": It is unclear what the objective of cooperation is, with respect to "addressing incidents". The DPA has no incident response capacity. The DPA notification requirement concerning incidents, involving personal data, are already in place.

Article 29 (Supervision and enforcement for essential entities):

- case-by-case: Could the Commission please confirm, that the main aim of Article 29 is to ensure, that the competent authorities are granted the necessary powers to perform audits, checks, controls etc. as specified, but that the actual planning, conduct and regularity of the aforesaid etc. are to be decided on a case-by-case basis by the competent authority being responsible for supervision of the specific essential (or important) entity?
- (4)(h) making aspects of non-compliance public: Is the intention that the entities should publish matters regarding their cyber vulnerabilities? Could the Commission elaborate on the pros and cons of such decision, and the rationale behind ultimately including such a provision?
- (8) detailed reasonings: Is the requirement for the competent authority to set out detailed reasoning for its enforcement decisions, to be considered a sort of reporting or transparency requirement? Ie. does the competent authority have to make such reasonings public or submit them to a central coordinating body - or is the point of this requirement to protect the audited entity and to make the reasonings available to them?

Article 29 & 30

- methology / established standards: What is the methodology of these requirements? Do they derive from established standards?
- preclude the publishing of significant incidents: Do the provisions preclude MS's from requiring that significant incidents be published as part of the published annual report?
- "security scans": According to **Article 29, paragraph 2(d)** and **Article 30, paragraph 2(c)** Member States have the power to subject essential entities to "security scans" based on objective, non-discriminatory, fair and transparent risk assessment criteria. What does a security scan entail?
- need for capability to advise on diagnosing and operational handling: Is it so that **Article 29, paragraph 4(e)** and **Article 30, paragraph 4(e)** presuppose that entities, in addition to protecting themselves according to the obligations, also need to be capable of advising on diagnosing and operational handling of cyber incidents? (And if so, can they be expected to have the capacity to lift these obligations?)

Article 30 (Supervision and enforcement for important entities):

- (4)(i) freedom of choice: As the legal system of DK does not provide for administrative fines (e.g. reflected in the national implementation of Directive 95/46/EC concerning data protection), could the Commission confirm our interpretation of this article, as including a freedom of choice with respect to its national implementation?

Article 31 (General conditions for imposing administrative fines on essential and important entities):

- (4) limits: It is difficult to understand the intention of the wording "maximum" and "at least" in the same sentence. Are the MS required to set a maximum limit, and not a minimum limit, for fines? Does the ceiling for this fine need to be at least 10 000 000 EUR?

fines shifted on to the consumers: ~~In some cases (e.g. revenue-regulated entities in the DK energy sector) there would be no other way to legally cover the costs associated with administrative fines, than ultimately shifting them onto the consumers through increase in (energy) prices. Could the Commission share its thoughts concerning this scenario?~~ **It should be a focal point that the framework for administrative fines ensures proportionality in order to preserve among others security of energy supply and avoid shifting of large economic burdens onto the consumers. Could the Commission share its thought on this?**

Article 33 (Penalties):

- sanctions: With respect to sanctions, it is the Danish view that focusing on sanctions/penalties should not be preferred as a means to ensuring compliance. MS's have different approaches, and equal weight should be given to stipulating a certain level of public-private partnerships, ISAC's or other cooperative measures as means to disseminate knowledge and acceptance of security considerations and thus to ensure compliance. Work in cyber security requires trust and cooperation.

Article 34 (Mutual assistance):

- (1)(b) mutual assistance / inquiries from other MS: Could the Commission please elaborate on how inquiries from other MS should be handled, if a situation arises where the competent authority is unable to fulfill its obligation (e.g. volume of inquiries exceeding the allocated resources of the competent authority)?

FINLAND

Preliminary comments and questions:

Article 24

Art. 24 (1): Would this entail that the supervision of DNS service providers would be only effectuated from the MS where the main establishment is located? If so, could lex specialis be considered as an option for DNS service providers to avoid possible discrepancies in supervision of DNS service providers between MS?

Art. 24 (2): In regards group companies, would jurisdiction concern only the main establishment of the parent company, even if subsidiaries would offer partly different services than the parent company?

Article 25

Art 25 (1): In addition to the information to be submitted, should entities provide information on the type of service(s) they provide?

Also, would ENISA or national competent authorities review this information to ensure that entities have accurately interpreted their role/services from the point of view of the directive?

Should entities also inform in which Member States they provide their services? Should this information be forwarded to each Member States' SPOCs?

Art 25 (4) is an important addition to ensure the supervision of entities.

Article 26

Art 26 (1): How can Member States ensure in practice that entities are exchanging relevant cybersecurity information among themselves? Is the goal to ensure the prerequisites for this or should authorities ensure in practice that information is actually exchanged? Should Member States provide platforms for this and is this exchange of information meant to be only between entities or can national competent authorities or CSIRTs participate?

Art 26 (4): Could a mandatory notification ("shall") induce excessive administrative burden for both entities and supervising authorities?

In general, could art. 26 be formulated more as a recommendation encouraging information-sharing arrangements?

Article 27

We support continuing the possibility for voluntary notification. "When processing notifications, Member States shall act in accordance with the procedure laid down in article 20 " – this wording should be further clarified (what does the procedure entail in this context?).

Article 28

Art. 28 (2): Could the Commission clarify on this cooperation in practice, is this cooperation reciprocal?

Article 29

Art. 29 (2) (a): Could the Commission elaborate on how on-site inspections should be effectuated in a situation (according to art. 24 (1) where an entity provides services in different Member States but would be under the jurisdiction of one MS?

Art. 29 (2) (b): what would regular audits include in more detail?

Art. 29 (2) (c): what is the difference between regular audits (b) and targeted security audits (c)?

Art. 29 (2) (d): security scans should be further clarified (definition, goal, roles and responsibilities between competent authorities and entities). For example, would security scans include network scanning, port scanning, vulnerability scanning?

Art. 29 (2) (e): Should Member States ensure that entities according to art. 24 (1) comply with the notification obligations according to art. 25 (1) and (2)? (While the registry would be maintained by ENISA)

Art. 29 (2) (g): Would the criteria for security audits and the qualifications of the auditor be at the discretion of Member States?

Art. 29 (4) (g): Could the Commission clarify the role of the officer?

Art. 29 (6): How should this be arranged in practice?

Article 32

To avoid overlapping provisions, the wording of this article could be adjusted to include a reference to provisions in GDPR.

Article 33

Could the Commission clarify art. 33 and its relation to art. 28-31, are penalties according to art. 33 overlapping with provisions in art. 31? In general, we highlight the need for national leeway regarding penalties and administrative fines (the sanctions system as a whole).

HUNGARY

Article 24 - Jurisdiction and territoriality
We are interested in the reasons why the Commission considered it necessary to amend the rules on jurisdiction.
Digital service providers under Article 24 (1) typically have infrastructure in several Member States. It therefore arises whether the competent authority determined in accordance with Article 24 is also entitled to carry out on-site inspections under Article 29 (2) (a) or only the Member State where the service provider infrastructure is located. How can on-the-spot checks be carried out in a Member State other than the competent authority in accordance with Article 24? Can "remote control" under Article 29 (2) (a) in such cases include cross-border control?

Article 25 - Registry for essential and important entities
We would like to know more about why the Commission considers it necessary to set up a central register of digital service providers, maintained by ENISA.

Article 27 - Voluntary notification of relevant information
NIS2 provides for the handling of near misses by the competent national authority or CSIRT and extends the exchange of information between Member States to near misses. Under Article 11 (2), Member States are therefore required to ensure that their competent authorities or CSIRTs are notified, in addition to events and cyber threats, of near misses "reported under this Directive". Pursuant to paragraph 3, competent authorities or CSIRTs must also inform the SPOC of incidents, cyber threats and near misses. Pursuant to Article 12 (4) (b) and Article 13 (3) (b), Member States shall also exchange information on near misses in the framework of the NIS Cooperation Group and the CSIRT Network. In accordance with Article 20 (9), the SPOC's monthly report shall also contain anonymous and aggregated data relating thereto. However, the reporting obligations of essential and important entities under Article 20 do not cover near misses and are not mentioned in Article 26 on cyber security information-sharing arrangements. The possibility to report near misses is only provided for in Article 27 on the voluntary reporting, but this article applies to organizations outside the scope of NIS2. We wonder why the reporting of near misses has not been included in the Article 20 or Article 26. Why is it included in Article 27, which deals only with actors outside the scope of the NIS? How will national authorities and CSIRTs become aware of such events?

Article 34 – Mutual assistance
How does the Commission envisage in practice a procedure under Article 34 (3) (c)? Why is it needed for Member States to consult ENISA and the Commission in particular?

Article 37 - Committee procedure
NIS 1.0 included a deadline for the adoption of implementing acts or the submission of its first draft. Does the Commission intend to add deadlines to NIS 2.0 in a similar way?

IRELAND

Article 24

24.1 Why is the concept of "Member State of main establishment" limited to the specified categories of digital infrastructure? Why is the concept not extended to all types of entity in the digital infrastructure sector?

24.2 Why has the criteria for "Member State of main establishment" been changed from "head office" to "decisions related to cybersecurity risk management measures are taken" or "establishment with the highest number of employees in the Union"? A reasoning for the change in the criteria is requested. Can the Commission also comment as to whether this change has any material effect, since ultimately the decision on choice of "Member State of main establishment" will be taken by these multinational companies? Who can argue with them as to where their decision making takes place or where they have their highest number of employees?

There is also the issue of subsidiaries, what if the overall company cyber risk management decisions are taken at company A, but its subsidiary is providing the service and company A may not exist in the EU? Again, what services deemed critical may vary from Member State to Member State depending on the offering, competition, etc., so how would this work?

24.3 Can the Commission comment further on the reasoning for Member States being empowered to take legal action against entities for failing to designate a representative? Has there been indications of non compliance? Does the Commission not have the power to take legal action or is this an exclusive competence reserved to Member States?

How could this work in practice? The representative to be held legally responsible for actions for another, extra jurisdiction entity, that they have no control over and are subservient to? Again, what about different services being offered in different Member States, how could this representative, outside a Member State jurisdiction be responsible.

Article 25

25.1 What is the purpose of the registry? Is it for transparency and information exchange? If so, why is the registry not a matter of public record and not publicly accessible?

Why is there not information on the types of entity that are applicable to the legal person concerned? Would an organization need to submit multiple entries to ENISA for the registry, with each entry referring to a particular type of entity?

Why is the deadline for submission not aligned with the transposition deadline for this Directive?

25.3 Why is there an obligation on ENISA to forward the information to Member States? Should the Member States not have the right to view the ENISA registry?

Article 26

26.1 Can essential and important entities share personal data as part of information sharing arrangements? If so, what provisions of the GDPR can the entities rely upon? Does this constitute a legal obligation (Article 6.1.c –GDPR) or performance of a task in the public interest (Article 6.1.e – GDPR)? Can the Council Legal Service comment in regard to this matter?

26.2 What is meant by "trusted communities of essential and important entities"? Are suppliers and vendors excluded? What about involvement of competent authorities and CSIRTs?

What is meant by "information sharing arrangements"? Can the Commission comment on scope of and number of such arrangements? Are they sector based, thematic based etc? Are they within Member States or can they be cross border? How many such arrangements should be established per Member State?

26.3 How will such arrangements be compatible with competition law? What is meant by "Member States shall offer support to the application of such arrangements"? Why type of support is envisaged? Financial, tools?

26.4 Are competent authorities to have a list of 'participating' essential and important entities in such information sharing arrangements? Is participation not mandatory for these entities? Is there not a danger of 'silent' or passive 'participation', where such entities will join such arrangements but not share any information?

26.5 Why is the phrase "In compliance with Union law" added? Is it possible that ENISA would provide support that conflicts with EU law?

Article 27

Why are voluntary notifications limited to 'significant incidents' only, in contrast to the situation where any 'cyber threat' or 'near miss' can be reported?

What is meant by "the procedure laid down in Article 20"? What specific paragraphs of Article 20 are relevant? Is this solely about the procedure of a notification referenced with implementing acts in paragraph 11 of Article 20?

Article 28

What is the purpose of this Article?

28.1 What is meant by 'effectively monitor'? Does this imply a general duty of surveillance of essential and important entities? Who, what, how is effective determined or measured? Who, what, how are "measures necessary" determined or measured? Who, what, how is compliance measured? Are competent authorities now going to mandate risk appetite of commercial businesses? Does this imply a general duty of intrusive surveillance and imposition of directed security governance of essential and important entities by the competent authorities (is that the intent in Article 29)?

28.2 What does "shall work in close cooperation with" actually mean? Is this a duty for competent authorities to cooperate with data protection authorities? What should that 'cooperation' be in practical terms and why is there not a reciprocal obligation on data protection authorities?

Article 29

Can the Commission outline the reasoning for the highly granular approach to supervision and enforcement set out in this Article? In particular do many of the enforcement measures not rely on a prior determination of a judicial authority before actions can be taken by a competent authority? Are such measures, in so far as they relate to natural persons, consistent with Fundamental Rights?

Who is determining local risk appetite in a commercial business and taking that into account? How is any of this supervision and enforcement supposed to be achievable with entities mainly located or providing services from non-EU countries like the UK?

29.1 Does this mean that the measures need to be adopted to each individual case? What is an 'individual case'? Does it refer to a particular entity or a particular infringement by that particular entity?

29.2 In regard to supervisory tasks and powers, the following queries arise:

1. What is meant by 'on site inspections' and 'off-site supervision'? Are such inspections to be undertaken unannounced and without notice? What precisely is to be inspected – equipment, facilities, staff, procedures etc? What is meant by off-site supervision-access to documentation, interviews of staff, information exchange with sectoral regulators?

2. What are 'regular audits'? Is this about generic information security compliance auditing in accordance with standards such as ISO/IEC 27007? What is meant by regular –periodic security assessments and pen testing? What is the scope of such audits –the organization, the NIS, specific systems, software?

3. What is meant by 'targeted security audits'? How do they differ from 'regular audits'? Are they undertaken by staff or are they organized by external parties?

4. Who undertakes the 'security scans'? What are they? URL scans, port scans, passive monitoring? What about liability implications arising from business disruption from a scan on an OT network?

5. What is meant by "to assess the cybersecurity measures adopted by the entity"? Is it the role of the supervising authority to undertake risk management of the supervised entity? There is a difference between having an opinion on adequacy of cybersecurity measures and determining what specific cybersecurity measures are appropriate based on the risk.

6. What is meant by 'evidence of implementation of cybersecurity policies' and 'underlying evidence'? Given that the evidential standard of proof can be interpreted to be that which satisfies a Court of law and can therefore be very onerous, is use of the word 'evidence' appropriate? What is meant by 'qualified auditor'? Is this a reference to the need to ensure that the person and or organization has appropriate industry certifications?

29.3 Why are the obligations on the supervising competent authorities as regards purpose and specification only limited to requests and not also activities set out in Article 29.2.a to d?

29.4 As regards the enforcement powers proposed the following questions arise:

1. What is meant by 'warnings'? Are these to be documented or can such warnings be verbal only? Who determines 'non-compliance with the obligations'? Is this the mere opinion of the competent authority or a finding of a Court of law?

2. What is meant by 'binding instructions'? Are these detailed prescriptive measures which must be precisely followed? If so, is the competent authority accepting civil liability? Who determines that there are deficiencies and that there have been infringements of the obligations? Is this for a Court of law to determine as opposed to an opinion of a competent authority? An 'order' is generally a matter for a judicial authority or a Court of law not an administrative body such as a competent authority?

3. A determination on 'conduct that is non-compliant with the obligations laid down in the Directive' can only be made by a Court of law? Would a competent authority not need to await such a finding from a judicial authority before issuing such an order otherwise it is likely that the competent authority could be found to be acting '*ultra vires*'?

4. As the previous case, any order could only be issued after a finding of non compliance with the obligations. Is the Commission inferring that a competent authority can act in a judicial capacity?

5. What is meant by 'protective or remedial measures'? Who assumes liability for this 'order', the essential entity or the competent authority?

6. What is meant by designating a 'monitoring officer'? Is this a member of staff of the competent authority, an external agent of the competent authority or a staff member/agent of the essential entity?

7. As regards publication of non-compliance, why would an entity agree to such a measure? Would it not be for a judicial authority to determine non-compliance and the scope of that for such an order?

8. What is the reasoning behind a public statement being made by a competent authority identifying a person responsible for an infringement? Would such an action have to await a prior determination by a judicial authority on whether such an infringement took place? What about Fundamental Rights and the rule of law, especially in regard to natural persons?

9. What is the reasoning for the administrative fine being an alternative to all other enforcement measures in Article 29.4?

29.5 What is meant by 'prove ineffective'? Enforcement actions can take time, perhaps many years especially when judicial authorities are involved. A determination that an infringement exists can take months and even years when Courts are involved.

What is meant by a 'certification or authorization body'? Competent authorities would not have any powers to overrule other public authorities without recourse to judicial authorities for such an order.

It is not clear whether the suspension of a service provided by an essential entity would be considered proportionate in law by judicial authorities. Is there any case law from the Courts of Justice in regard to this matter?

What is meant by "temporary ban against any person discharging managerial responsibilities" and of "any other natural person held responsible for the breach from exercising managerial functions"? Would not holding individuals to account not require determinations by judicial authorities? Authorities with experience in corporate enforcement, would have the appropriate expertise and competence to bring matters before Courts for determination. The individuals concerned also have Fundamental Rights?

Has the views of the Fundamental Rights Agency been sought in regard to this legislative proposal?

How could such measures be applied to public administrations, in particular ministries, without impacting on the constitutional order of individual Member States?

29.6 How can Member States ensure that those natural persons who exercise control of an essential entity can be held liable for breach of their duties as regards compliance with the obligations laid down in the Directive? What happened if such control is exercised by a group of individuals acting collectively as for example, a Board of Directors? Who then is responsible –all Members of the Board, including non-executive Directors?

29.7 As regards taking various factors into account, the following queries arise:

1. What is meant by 'serious disruptive effect'? Is this a very public loss of availability, integrity and/or confidentiality of the underlying network and information system under pinning the entity's function?

2. What is meant by 'obstruction of audits' and 'false or grossly inaccurate information'? Is this not for a judicial authority to determine before any reliance can be made on these non objective factors?

3. What is meant by 'intentional or negligent character of the infringement'? Is this not for a Court to determine?

29.8 What is meant by 'detailed reasoning'? Can some examples be given, even in the abstract? Would not the sharing of preliminary findings lead to a situation where the essential entity seeks recourse to judicial authorities to vindicate it's rights?

29.9 Can the Commission clarify precisely when the CER competent authorities need to be informed? Is this before or after the essential entity has notice of supervision and enforcement activities?

What precisely is meant by the last sentence? It can be interpreted in two very different ways. Do the NIS2 competent authorities need proactive approval of CER competent authorities (i.e. upon request…) before supervision and enforcement measures can be taken on an essential entity that is a critical or equivalent to a critical entity in CER? Alternatively NIS2 competent authorities take supervisory and enforcement measures at the instigation of the CER competent authorities on an essential entity that is a critical or equivalent to a critical entity in CER?

Article 30

30.1 What precisely is meant by "When provided with evidence or indication …"? The word 'evidence' would set a very high benchmark equivalent to a finding of a Court of law. What would 'indication' mean? Is it merely an assertion or must it be some empirical data (e.g. audit report) , witness testimony or considered opinion in writing from a public body in a Member State?

30.2. It is noted that supervisory tasks exclude provision for compliance audits and also for reports of implementation of cybersecurity policies. Why does this differ from supervisory tasks on essential entities since such additional aspects could also be ex-poste in their characteristics?

30.3 Why do the purpose and specification requirements not apply to all supervision tasks?

30.4 As regards the enforcement powers proposed the following questions arise:

1. What is meant by 'warnings'? Are these to be documented or can such warnings be verbal only? Who determines 'non-compliance with the obligations'? Is this the mere opinion of the competent authority or a finding of a Court of law?

2. What is meant by 'binding instructions'? Are these detailed prescriptive measures which must be precisely followed? If so, is the competent authority accepting civil liability? Who determines that there are deficiencies and that there have been infringements of the obligations? Is this for a Court of law to determine as opposed to an opinion of a competent authority? An 'order' is generally a matter for a judicial authority or a Court of law not an administrative body such as a competent authority?

3. A determination on 'conduct that is non-compliant with the obligations laid down in the Directive' can only be made by a Court of law? Would a competent authority not need to await such a finding from a judicial authority before issuing such an order otherwise it is likely that the competent authority could be found to be acting '*ultra vires*'?

4. As the previous case, any order could only be issued after a finding of non compliance with the obligations. Is the Commission inferring that a competent authority can act in a judicial capacity?

5. What is meant by 'protective or remedial measures'? Who assumes liability for this 'order', the important entity or the competent authority?

6. As regards publication of non-compliance, why would an entity agree to such a measure? Would it not be for a judicial authority to determine non-compliance and the scope of that for such an order?

7. What is the reasoning behind a public statement being made by a competent authority identifying a person responsible for an infringement? Would such an action have to await a prior determination by a judicial authority on whether such an infringement took place? What about Fundamental Rights and the rule of law, especially in regard to natural persons?

8. What is the reasoning for the administrative fine being an alternative to all other enforcement measures in Article 30.4?

30.5 Article 29.6 to 8 refer to 'essential entities' and not 'important entities'. Why, in the interests of drafting accuracy, have the respective paragraphs been omitted?

Article 31

Why is there such a fixation with penalties? Is there an expectation of systematic non-compliance?

31.1 What is meant by 'effective, proportionate and dissuasive'? Is there any Court of Justice case law to assist in further interpreting these relatively vague principles? It has to be recognized that they can be interpreted very differently by judicial authorities in the different Member States.

31.2 With the exception of the reference to Article 29.5, is this provision not merely repeating what is in Article 29.4.j and Article 30.4.i?

31.5 What is meant by 'periodic penalty payments'? Can they in effect refer to instalment payments of administrative fines? If not, what are they referring to? What is meant by 'prior decision of the competent authority'?

31.6 What is the thinking behind this provision? Is it therefore possible to have a nominal administrative fine imposed on public administration entities?

Article 32

Why is this provision needed in this Directive?

32.1 Why is there a lack of reciprocity as regards the obligation on NIS competent authorities to inform the GDPR supervisory authorities of personal data breaches arising from infringements under Article 18 and 20 of this Directive? It is not clear as to how the competent authorities become aware of a definitive data breach if they are not legally competent to determine same. Why is this provision needed since the obligation should be on the relevant entity to report a data breach?

32.2 Why should NIS competent authorities not be able to impose administrative fines? What is meant by 'same infringement'? How could an infringement under GDPR be the same as an infringement under NIS2, even if it is derived from one common event?

Article 33

What is meant by penalties as distinct from administrative fines? Can such enforcement measures include legal proceedings under criminal law to fine and imprison individuals?

Article 34

Can the Commission explain what is intended with this provision?

34.1 Is this provision about mandatory cooperation between competent authorities in different Member States? In particular the following queries arise:

1. The obligation to inform and consult with other relevant competent authorities by the competent authority applying supervisory and enforcement measures is noted. However, the provision is silent as to when this information exchange should take place. As regards supervision, should the information exchange take place prior to, during or after the tasks take place? On the question of enforcement should the detailed reasoning under Article 29.8 be shared with the relevant competent authorities, before or after this has been sent to the essential or important entity in question? What are the liability implications? How can confidentiality be ensured? What about constraints introduced by national judicial processes i.e. Courts on information exchange?

2. It is noted that a request to take supervisory and enforcement measures may be made to another competent authority in a different Member State. However while there may be some scope for such practical cooperation with supervisory tasks, effective enforcement generally involves the legal and judicial processes of the different Member States. It is not clear as to whether one competent authority could act as an enforcement agent for an authority in a different Member State without application to its national Courts. What if a competent authority is asked to rely on the findings of a peer competent authority in another Member State to undertake enforcement actions, in circumstances where due diligence and due process to the standards expected by the Courts in its own Member State have not been met?

3. What is meant by a 'justified request'? Who decides? The Courts of the relevant Member States or ultimately the European Court of Justice? Who decides as to whether "the authority is not competent to provide the requested assistance" or that the requested assistance is not proportionate to the supervisory tasks? Who is liable and what are the risks involved if supervision tasks undertaken by an agent competent authority are less than satisfactory? Would there not need to be a collective, perhaps even uniform, understanding as to what "on site inspections", "off site supervision" and "targeted security audits" are?

34.2 What precisely are "joint supervisory actions"? Under what type of circumstances would such a scenario take place? Are there preexisting examples of such an approach in other areas of regulation in the EU Internal Market?

ITALY

Art. 25, par. 1 and 4.

- What are the reasons why ENISA shall create and maintain a registry for essential and important entities referred to in art. 24, par. 1 (DNS service providers, TLD name registries, cloud computing service providers, etc)?
- Could national security or other relevant considerations prevent Member States to allow essential and important entities referred in art. 24, par. 1, to communicate to ENISA the details to be included in the registry? If so, would such entities be exempted from communicating the required information?
- In light of par. 4 which prescribes Member States to ensure the concerned entity's compliance with the obligations laid down in the Directive, why are the entities in charge of submitting the information to ENISA and is it not up to the Member States?

Art. 26, par. 2 and 3.

- Does the Commission imply that essential and important entities form "per se" and become "automatically" part of "trusted communities?" Can they establish "inner circles" of information sharing?
- Is the involvement of "public authorities" in the concerned arrangements mandatory or voluntary?
- What kind of support should Member States exactly offer to the application of such arrangements?

Art. 27

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

Art. 29, par 2(d) and Art. 30, par. 2(c).

- What the exact meaning of "security scan" referred in both articles?
- Does the expression include the power of national competent authorities to impose penetration tests or other thorough scrutiny or tests upon essential and important entities' networks, systems or services?

Art. 29, par. 2(e)

- Since national competent authorities should have the power to requests information that are necessary to assess compliance with the obligation to notify the ENISA pursuant to Article 25(1), would not make more sense that the responsibility to communicate art. 25(1) relative information is attributed to these authorities?

Art. 29, par. 4(h)(i) and Art. 30, par. 4(g)(h).

- Taken in to account the general goal of promoting the enforcement of the Directive's provisions, are there any further and specific reasons why national competent authorities shall have the power to order essential and important entities to "make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner"?
- Furthermore, what are the reasons why national competent authorities shall have the power to "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"?
- Have the Commission considered that the underlining "naming and shaming" approach could be non-proportionate to the general goal of promoting the enforcement of the Directive's provisions?

Art. 29, par. 9.

- Is there any reason why – when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical – competent authorities under the NIS Directive should inform the competent authorities under the CER Directive and not also vice-versa? Why is this duty of information not foreseen on reciprocal basis?

Art. 31, par. 4.

- Has the Commission taken in to account the "proportionality" of the administrative sanctions regime?
- Does the Commission not consider the maximum amount of the administrative sanctions being non-proportionate to the pursued goal of ensuring the enforcement of the Directive's provisions?
- Has the Commission considered the potential impact of such a high amount of sanctions on essential and important entities (especially medium size entities)?
- Has the Commission considered that, in some Member States the establishment of the maximum amount of an administrative fine will also affect/impact on the determination of the minimum amount of the fine and this will require Member States to entirely recalibrate their sanction regime?

Art. 33, par. 1.

- What is the exact meaning of "penalties"? According to recital 74, the term also includes punishment under criminal law, doesn't it?

Art. 34, par. 1(c) e 2.

- Does the provision of mutual assistance established by the article require the competent authorities to provide information that are covered by national or public security to other competent authorities?
- Could Member States exempt their competent authorities to follow up requests of mutual assistance which are in conflict with their interest of national or public security?
- Given the characteristics and peculiarities of domestic jurisdictions, has the Commission considered that the possibility for competent authorities from different Member States to carry out joint supervisory actions can be quite limited in practice?

LATVIA

Article 24:

- Why the entities providing domain name registration services for the TLD (so-called registrars) isn't included in this article?
- Definition of the term "*main establishment*" should be aligned with the definition in GDPR Article 4(16). Otherwise it may cause unnecessary ambiguity both for the supervisory authorities and entities under NIS2.
- Para3 and 4: In accordance with Article 2(2) NIS2 requirements will apply to some of these subjects disregarding its size. It may be a too big burden for smaller companies which may cause that they would simply withdraw from EU market. Don't you see a danger that the proposed NIS2 scope may encourage development of "splinternet" in EU level?

Article 25:

- Para6: Who would ensure that each company registers its data? Who would maintain the list of registry users? Who would control the quality of the data in the registry? Are there any further guidelines planned in this regard?
- Can you elaborate on the relations between ENISA and EC registers? Have you considered the risk of fragmentation of the information with regard of these two registers?

Article 26:

- When ENISA guidelines are planned?
- How to ensure fulfilment of GDPR requirements?
- Can you elaborate on "*exchange of information takes place within trusted communities*" in para2? Can information exchange be ensured through CERTs?
- What is the intended aim of informing mentioned in para4?

Article 27:

- We fully support CERT.AT opinion: "*This should be a bit more generic. This article needs also to cover: 1) non-covered entities reporting incidents and vulnerabilities / risks on their side 2) anybody reporting incidents / vulnerabilities / risks detected anywhere else. Why is that important? We used to get a data-feed from Google covering issues with web-pages their crawler detected in the Austrian Internet. They stopped providing this, claiming problems with the GDPR. It would be really helpful if security researchers have a clear greenlight to report their findings to the national CSIRTs.*"
- Which specific procedures form Article 20 would be applicable here?

Article 28:

- Can you elaborate on how you see the practical supervision of this requirement? Will the supervisory tools be developed centralised (in EU level) or this will remain the responsibility of each MS?

Article 29:

- How often and to what extent (scope) these inspections should be carried out? Can any guidelines from ENISA be expected (if yes, when)?
- Para4(h): Should publication obligation be applicable in all cases?
- Para5(a) should state what kind of certificate would be subtracted and para 5(b) should be more specific in describing to which employee specifically this can be applied.
- Para6: We have concerns on how ENISA would ensure that all date in the registry is up to date.
- What is meant by "*sanctions*" in Para7?

Article 30:

- Para4(h): Should publication obligation be applicable in all cases?

Article 31:

- We would consider that sanctions should be the last resort if the other measures (Article 29(4)) haven't worked. Para2 in Article 31 currently doesn't reflect this approach.
- Para4: We don't believe that consequences of the failure to inform about the incident in all cases would require application of sanctions. Proportionality principle should be taken into account.
- Can you elaborate more on Para5? An example could bring more clarity.

Article 32:

- We would expect some EU guidelines in this regard.

Article 34:

- Will there be a common information exchange system in EU level? Which requirements will be inspected?

LITHUANIA

Initial points of clarification in regards to Articles 24-34 of NIS 2 Proposal

Disclaimer:

The following questions in relation to Articles 24-34 of the Proposal are non-exhaustive and might further be expanded.

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

Comments and Points of clarification:

Article 24.3:
Should the absence of established representative in one of the Member States where the services of the entity are offered be considered as non-compliance with the obligations under this Directive?

Article 24.3:
In the absence of a designated representative within the Union, what would happen in case where two or more Member States take legal actions against the entity for non-compliance with the obligations under this Directive?

Article 25.4:
Can you explain the meaning of "shall be competent to ensure that entity's compliance with the obligations laid down in this Directive"?

Article 26.2:
What should be the meaning of "trusted communities"? What makes a community of essential and important entities *trusted*?

Article 26.5:
Would it be possible to give some of the best practices/ examples of such cybersecurity information-sharing arrangements to have a better understanding at this stage?

Article 27:
If Member States, when processing voluntary notifications, shall act in accordance with the procedure laid down in Article 20, does that mean that the competent national authorities shall provide a response to the notifying entity, including initial feedback on the incident, within 24 hours, and, upon request, further guidance?

Article 27:
Would eliminating the vulnerabilities/ causes for cyber incident be considered as additional obligations upon the reporting entity, which it would not have been subject had it not submitted the notification?

Article 28.1:
Can you elaborate on the meaning of "effective monitoring"?

Article 29.1:
In relation to paragraphs 2 and 4, could you give examples of particular cases where certain supervision and enforcement measures would be effective, proportionate and dissuasive?

Article 29.5/ 29.6:
How should that be conducted in case of public administration?

Article 30.2:
Can national competent authorities go beyond or choose different measures from the listed ones?

Article 31:
On the one hand, the potential amount of administrative fines is very high (para 4), on the other hand, circumstances of receiving such fines seem to be very vague and dependent on the decision of national competent authorities (paras 2, 3 and 6). To ensure transparency and sense of fairness, the more clarity in this regard, the better.

Article 32.1:
What is a *reasonable* time frame? Why the timeframe of 72 hours is taken out?

Article 33.1:
Could you elaborate further on the requirement for Member States to lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive?

LUXEMBOURG

Article 24

Regarding the jurisdiction and territoriality defined in the NIS2.0 with respect to TLD, DNS, and digital providers, and regarding the possibility for those entities to be defined as entities equivalent to critical in the context of CER, Luxembourg wonders if under CER the same territoriality provisions will be considered? Or might it actually happen that more MS define one digital provider equivalent to critical in CER?

In Article 7 of CER, cloud computing service providers could be designated by MS as "entities equivalent to critical entities". However Article 1 point 2 says that the CER will not apply to matters covered by the NIS2.0. Considering that cloud provider will be under the jurisdiction of one MS for NIS2.0, but potentially under the jurisdiction of more than one MS under CER except for cybersecurity issues, would those MS need to contact the CA of the MS where that provider is considered essential under NIS2.0 to get information about their cybersecurity obligations?

Article 26

Concerning Article 26.4, we would like to know whether this could be part of the peer-review foreseen in Article 16, and thus if this would not potentially render this notification obligation unnecessary?

Article 29

For points (c) and (d) of article 29.2, does that mean the CA can request the entity to perform security audits and security scans? Or does that mean that the CA can perform these activities itself on the entity?

SLOVENIA

Article 25
Is the text as currently proposed sufficient for the authorities of those Member States which (as incompetent under the rules of Article 24) have not been informed of anything through their 'single points of contact' by ENISA? Would it be beneficial also for ENISA to notify also the 'single points of contact' of other Member States, which are not covered by Para 3 of this Article – also from the perspective of the Article 34?

Article 26
We ask for further clarity on Para 2 with regard to the "exchange of information takes place within trusted communities of essential and important entities". What is meant by "trusted communities of essential and important entities"? Who determines that they are not trusted or that they are trusted? Is it foreseen to work on the minimum common criteria or recommendation (similar to the 5G Toolbox)?

With regard to the Para 3 we are concerned about the possible disproportionate (administrative) burden on Member States. What is meant by the "involvement of public authorities in such arrangements" and by "operational elements, including the use of dedicated IT platforms"? What is meant in the last sentence of Para 3 with "shall offer support"?

Article 28
Proposal of Article 28 obliges the competent authorities to cooperate with data protection authorities. We would welcome more clarity on responsibilities, scope and manner of cooperation. The practice has shown that such interplay is difficult to define. In the field of electronic communication an attempt was made with the EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.

Article 33
Is the proposed deadline of two years from the Para 2 in line with the proposed deadline of 18 months for the transposition in Article 38?

Article 34
With regard to Article 34, is has already been pointed out under Article 25, the proposed regulation may be difficult to implement in practice if not all single points of contact have previously received at least some information from ENISA (under Article 25).

SPAIN

COMMENTS	JUSTIFICATION FOR THE SPANISH PROPOSAL
Article 24 Jurisdiction and territoriality	We welcome this point. Clearer criteria when determining the main establishment of an entity will help to prevent transnational entities from circumventing / hindering the supervisory work, or choosing the supervisory entity most favorable to their interests, generating a more homogeneous European supervisory framework.
Article 25 **Registry for essential and important entities**	We welcome the establishment of the Registry for essential and important entities. One of the main hurdles in the supervision of PSDs under the current NIS Directive has been that some PSDs have been reluctant to notify their existence to the PSD Supervisory Bodies, even in those Member States (e.g. Spain) where this notification was mandatory, even under menace of fines. Entities have been slow answering to prompts from the Supervisory Bodies, and have pleaded ignorance of this legal obligation. The Supervisory Bodies of several Member States have spent considerable time and money searching and investigating potential PSDs. We are afraid that the Registry will fail to achieve its goals if the essential and important entities do not carry out their obligations. How will the Commission and ENISA ensure that essential and important entities fulfill the notification and update obligations to the Registry? Will ENISA spend considerable time and money searching, investigating, and prompting potential essential and important entities that have not notified or updated? Will ENISA or the Commission prompt the Member States to impose fines on those essential and important entities that do not notify or update? Art. 25.2 states that essential and important entities must notify ENISA all initial and update data for the Registry for essential and important entities. Intermediate actors such as the competent authorities / supervisory bodies are not mentioned in this regard. This does not consider that in some Member States (e.g. Spain) some authorities will use the initiative to designate entities as important or essential. In the current proposal, if an entity is designated as NIS2, then it is this same designated entity who has to report to ENISA. It may be necessary to mention in this article that the notification of the information of essential and important entities can be made through the competent authority of the member states or the SPOCs. Do member states have to notify ENISA when they designate an entity? This point should be clarified. It is vital for the daily tasks of the Supervisory Bodies and CSIRTs to access this Registry, in order to provide the service and

	supervision that is due to each entity. By the time an incident or a request from an entity is received by a reference CSIRT, for example, it must be fully known what type of entity it is and what it is subject to, because the CSIRT's response must be in accordance with it. Member States should have greater access to the registry. The article should state directly that, in addition to notifying the corresponding member state of the entity, all SPOCs, CSIRTs and national authorities can have direct automatized access to the whole Registry for essential and important entities. In the part that mentions that ENISA will support the establishment of mechanisms and tools for the exchange of information on cybersecurity, the ISAC platforms could be explicitly mentioned as an example. In some Member States all current essential service operator are critical infrastructure operators. This information is secret according to our legislation. How will ENISA deal with this fact when managing the Registry?
Art. 26 **Cybersecurity information-sharing arrangements**	[Paragraph 1] The requirement that Member States ensure the exchange of relevant cybersecurity information between essential and important entities requires that: 1. Such exchange can be carried out automatically, through an sharing Node at the national level (section 3), in which all the essential and important designated entities must be recipients of the exchanged information, regardless of the sector they take part. 2. Likewise, the Competent Authorities, the reference CSIRTs and the SPOC must have access to the information exchanged (development of section 3). 3. Such exchange must be carried out over different networks, segregated and correctly secured, to avoid that a serious cyberattack could put at risk this exchange. [section 2] The Information Sharing Agreements are expressed in the article in an excessively general way. The best way to guarantee the suitability of such Information Sharing Agreements would be for NIS2 to force Member States to implement a national legal norm that regulates the recipients of such sharing Agreements, their content and their specificities. This would minimize the argument that certain entities could use to avoid the exchange of information, claiming risks for security, intellectual or industrial property, reputational damage, etc. Specific reference should be made to a common information exchange platform. Some functional requirements of this platform should be included.

	[section 5] The Best Practices and Guidance that the section entrusts to ENISA, to support the establishment of Sharing Agreements, could be supported, mutatis mutandis, on what is contained in the Spanish National Incident Notification Instruction. **Spain could make a proposal in this regard.** Also, the ISAC platforms could be explicitly mentioned as an example.
Art. 27. **Voluntary notification of relevant information**	Voluntary "near misses" reporting is a bit risky. It is necessary to specify more specifically what is meant by "near misses" to prevent an eventual avalanche of notifications of null or minor importance from preventing the normal development of the Information Sharing Node. In addition to this, a specific mention should be made within this article to collaboration between ISPs and national CSIRTs to effectively notify those incidents that affect their customers. For instance: To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation and coordination between the competent authorities single points of contact, CSIRTS and other entities in the national digital ecosystem as ISP, particularly regarding cyber threat and incident response
Art. 29 **Supervision and enforcement for essential entities**	The Spanish National Security Framework includes these obligations. Perhaps 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. 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.
	Deepen supply chain monitoring

Article 30 **Supervision and enforcement for important entities**	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
Article 31 **General conditions for imposing administrative fines on essential and important entities**	This article should explicitly mention that, although all Member States must comply with these requirements, they are free to impose further criteria.

SWEDEN

Article 24

The main rule of jurisdiction is stated in the recitation in recital 63 while the exceptions are stated in Article 24. Could the Commission explain why the exceptions to the main rule of jurisdiction is specified in a separate article and not in the main rule?

Article 24 (2)

How are competent authorities supposed to know where the decisions related to the cybersecurity risk management measures are taken? Are the entities supposed to inform the competent authority where these decisions are taken?

Article 25

SE would like the Commission to elaborate on the purpose of this register. This type of register has high protection values, how would safety issues and protecting measures be solved by ENISA?

Do the essential entities need to submit the same information to the competent authority as well or only to ENISA?

Article 26

Article 26 (1-2)

In this Article it is stated that Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves. SE would like the Commission to elaborate on what Member States must provide for such exchange of information to take place? What is meant by that exchange of information will take place within trusted communities and shall be implemented through information sharing arrangements in respect of the potently sensitive nature of information in Article 26 (2)? Does this Article refer to ICT platforms for such information exchanges to take place or does it refer to existing forums for information exchange?

This information will have a high protection value. How would safety issues and protecting measures be solved?

Article 26 (3)

Could the Commission explain what is meant by “public authorities”?

Article 28

SE would like the Commission to clarify what is meant by “reasonable period of time” in Article 28 (1).

Article 29

SE notes that the Article 29 is very detailed and comprehensive. SE is hesitant about the need for this level of detail in the proposal.

Article 29 (2 d)

SE would like the Commission to clarify the meaning of "security scans".

Article 29 (4 g)

It is stated that competent authorities have the power to designate a monitoring officer with well-defined tasks that will oversee the compliance with their obligations provided for by Article 18 and 20. Could the Commission explain the purpose of this and what it means in practice? What responsibility would the designated monitoring officer have and how would that relate to the responsibility of the management (as stated in Article 18)?

Article 29 (4 h-i)

SE would like the Commission to elaborate a bit more about the purpose of public statement and how this public statement would take place in practice. Public statement can be made in various ways – would it be up to the Member States to decide how this would go about?

Article 29 (7 d and g)

SE perceives writings in 7 (d) and 7 (g) to be arbitrary. How will the competent authorities take account of "the intentional or negligent character of the infringement" or "take account of the level of cooperation" as stated in 7 (g)?

Article 29.9

Could the Commission elaborate about the purpose of this Article and how this would work in practice?

Article 30

Could the Commission explain why the corresponding Article 29 (9) is not covered by this Article?

Article 33

In this article the Commission uses the term "penalties", whereas in article 31 "administrative fines" are used. Could the Commission explain why there are two different expressions used and why are there two separate articles on this matter?

Article 34

Could the Commission please elaborate on situations when Member States and competent authorities interpret the NIS-regulation in different manner?