Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 08 February 2021

WK 1627/2021 ADD 2

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI

WORKING PAPER

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 - Comments by CZ, DK, EL, LT, LU and PL

Delegations will find in Annex comments by CZ, DK, EL, LT, LU and PL on the above-mentioned subject.

TABLE OF CONTENT

CZECH REPUBLIC

ART. 1

As concerns the subject matter of the NIS 2, we observe that the **chapters III and IV of the NIS 2 are not included** in the Art. 1 para. 2. Why was a reference to these chapters not included?

ART. 2

Some entities that would fall into the scope of the NIS 2 provide more than one service and some of the services provided by such entities might not be related to the sectors listed in the Annexes I and II of the NIS 2. NIS 1 allows to distinguish between different type of services provided by one entity for the regulatory purposes. We don't see such flexibility in the NIS 2. In other words, **the regulated entities would be obliged to fulfil the cybersecurity requirements even in relation to the services not related to the services for which they would be actually regulated under NIS 2**. Can the Commission elaborate on its policy approach to this matter?

How did the Commission expect the **national authorities to get and stay informed about the entities under their jurisdiction** if the proposed self-identification model would be adopted? The proposal does not come with any provision on this matter. We are concerned that not only the competent authorities of MSs would lack information about entities under their jurisdiction, but also that entities falling into the scope of NIS 2 themselves would not be aware of their obligations (the latter applies particularly to important entities due to their minimal interaction with competent authorities).

While we are aware of the Commission's intention to allow the **MSs to identify the entities under the Article 2 para 2 points (c) to (g)**, this intention is not reflected in the text of the Art. 2 itself. We see this as a legislative shortcoming that brings uncertainty. Why was not this explicitly mentioned in the Article 2?

For what purpose needs the Commission to gather the **information on entities identified under the Art. 2 para. 2 points (b) to (f)**?

The practice of the implementation of the NIS 1 revealed an **uncertainty about whether some specific entities that provide digital services fall into the scope** of NIS 1 or not. An example of such a problematic digital service provider is a metasearch engine (or aggregator) – search tool that uses another search engine's data to produce its own results from the Internet (see WS DPS NIS CG working paper 3 on search engines). In our view, this shortcoming of NIS 1 was not addressed in the NIS 2 proposal. Did the Commission consider solving this matter in the NIS 2 in a harmonized way?

Analyzing possible future **interactions between DORA and NIS 2**, we found out that some entities falling into the scope of NIS 2, namely digital providers and digital infrastructure providers, might be also identified under DORA as ICT third-party service providers. If there were this overlap, how would NIS 2 interact with DORA in this matter?

DENMARK

In addition to the question sent yesterday, we would like the following questions to be additionally included in the forthcoming discussions:

Article 2:

- We have in the Danish energy sectors experiences an increase in creative business constructions which allows the companies to evade the scope of the directive. We therefore urge the EU COM to be mindful of this.

Article 2:

- As we understand the wording of Article 2, all government authorities, regardless of size and function, would be considered as "essential entities". Is this correct, and if so, could you please elaborate on why the proposal does not take into account differences in importance and function between entities belonging to the same category? Might it be considered to allow for "essential" and "important" entities within the same sectors as well as perhaps even the possibility of excluding some entities entirely from the scope of the directive?

Article 4:

- In relation to art. 4, no. 26, and annex II, the question arises if the consequences of using the definition of food business in regulation 178/2002 have been fully evaluated:

  According to the annex the scope of the proposal is i.a. food businesses as defined in regulation 178/2002. This would mean that the proposed regulation would cover a very broad group of businesses such as farmers and fishermen as well as wholesale or retail businesses where food is only a small part of the turnover e.g. a garden center with a very limited sale of candy. Furthermore, the definition is based on the physical business e.g. a slaughterhouse and not the company owning a number of slaughterhouses. The limitations in relation to size according to art. 2 would not solve those issues as a significant part of the Danish farmers and fishermen have an annual turnover in excess of 10 mio. Euro. In relation to especially retail there is at least in Denmark a substantial number of shops with a large turnover but a very limited sale of food.

GREECE

Art. 1

Art. 1 (2) (c): We propose the use of the wording "*rules and procedures*" instead of "*obligations*".

Art. 2

Art 2 (2): Instead of the submission of a list of entities to the Commission (currently the list of OES remains classified according to national legislation) we propose the use of the current phrasing of the art. 5 par.7 of NIS 1.0 (amended as necessary):

"*(c) the number of essential and important entities identified for each sector referred to in Annexes 1 and 2*".

- Art. 2 (3): We propose the preservation of the wording of art. 1 (6) of NIS 1.0: "*This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences*".

- Art. 2 (6): We consider that incident reports under the DORA regulation must be at least equivalent with the incident reports under the NIS 2.0. Furthermore, these incident reports concerning major ICT - related incidents should be obligatorily communicated not only to NCAs under DORA regulation, but also to the NIS SPOCs and/or CSIRTs (either directly by affected entities, or through the communication of the report per se to the competent authorities under the NIS 2.0). In addition, cooperation with the competent NIS SPOCs and CSIRTs in cases of major ICT - related incidents should be obligatory, and not at the discretion of the NCAs.

LITHUANIA

Initial comments and points of clarification from Lithuania

Disclaimer:

The following questions and comments in relation to Articles 1 and 2 of the proposal are non-exhaustive and might be further expanded.

Although current discussion is solely dedicated to the two Articles, certain sections (e.g. recitals) of the Proposal were added in Lithuania's comments for the sake of clarity and holistic view of the provisions.

Comments:

Article 2(1), with respect to proposed size cap rule: Taking into account the Commission's produced impact assessment of NIS Directive, which revealed significant discrepancies between EU Member States due to national identification processes of Operators of Essential Services (OES), Lithuania appreciates the proposed more harmonized criteria for determining, which entities should qualify under the scope of NIS 2. However, we also recognize the challenges that come with it, namely the large number of entities that will be affected by the Directive including the associated implementation burden (financial as well as human resources) they will face. Increased burden for NIS 2 national competent authorities should also be kept in mind. Following that, Lithuania would propose a more gradual approach to NIS 2 implementation through differentiation of implementation phases: first for large enterprises, following medium sized entities.

Article 2(2), with respect to micro and small entities: Emphasizing the importance of proportionality and seeking to minimize the associated burden on micro and small entities, which would fall under the scope of NIS 2, Lithuania would encourage issued guidelines on the implementation criteria applicable to micro and small enterprises, as mentioned in recital (10). We would also welcome further discussion on Commission's proposal for MS to share the list of such entities (in particular, ensurance of secure transmission and storage of such sensitive information).

Article 2(6), with respect to sector-specific acts: Lithuania strongly supports expressed MS views that NIS 2 should constitute a horizontal directive containing minimum security requirements across all sectors. For the sake of clarity, such requirements should also be specified. Whereas, in instances where provisions of NIS 2 do not apply to a specific sector, interaction between NIS 2 and sector-specific acts should be clear. To illustrate, currently incident reporting for financial sector entities raises questions, such as provision of feedback and support to cyber incident affected entity and interaction between DORA and NIS 2 competent authorities. In addition to that, Lithuania reiterates expressed concerns by Member States that DORA proposal is based on current NIS Directive and will be adopted before the agreement on NIS 2, which poses risks for inconsistencies. Aiming to ensure harmonization between the two instruments, more discussions should be held in common.

Points of clarification:

Article 2(2)(g), with respect to interaction with Resilience of Critical Entities Directive (CER): Article 2(2)(g) states that entities identified as critical or equivalent according to CER, will be within the scope of NIS 2, in turn, being subject to cybersecurity resilience obligations under NIS 2. Why then recital (14) states that request of competent authorities under CER is needed for competent authorities under NIS 2 to be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical?

Article 2(2)(d), with respect to public safety and public security: Could you, please, elaborate on the reasoning behind Article 2(2)(d) and Article 4(23): public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded from NIS 2 but all entities should be included under the scope of Directive if the potential disruption of the service provided by the entity could have an impact on public safety and security.

Article 2(2)(e), with respect to systematic risks: Could you elaborate on the meaning of "systematic risk"?

Article 2(2)(f), with respect to regional importance: Could you elaborate on the meaning of specific importance at regional level?

Article 2(2)(a)(i), with respect to correlation with the European Electronic Communications Code (EECC): Could you explain the correlation between NIS 2 and the EECC, also, taking into consideration obligations on cybersecurity information sharing, as stated in Article 1(2)(c)?

LUXEMBOURG

Article 1:

Art1.1: Luxembourg appreciates that the new proposal aligns with definitions from the cybersecurity act. However, it is necessary to define the extent of the subject matter more precisely. Considering that the new subject matter is defined as "ensuring a high common level of cybersecurity" and considering the definitions of "cybersecurity" and "cyber threat"[1], one could interpret that the physical integrity (e.g. damages resulting from incidents due to human error or any other physical damages) may not be in scope of the NIS 2.0 proposal.

As a result, Luxembourg proposes to further clarify the scope and suggests to also refer to the "security of network and information systems" in the subject matter of the new proposal. The European Commission explained that physical integrity would be in the scope of cybersecurity as it is included for example in the scope of the ISO 27005 standard. However, it should be pointed out that the title of that standard refers to information security risk management and not to cybersecurity risk management.

In the same vein, the European Commission could further elaborate on the relation and potential overlap of the NIS 2.0 proposal and the proposal for a directive on the resilience of critical entities.

Finally, we noticed that Art1.1 does not include any reference to improving the functioning of the internal market. Hence, Luxembourg suggests to also include wording to what extent the new proposal contributes to deepening the single market.

Article 2:

Art2.1: In light of the explanations given by the European Commission, we understand that the new proposal applies to ALL public and private entities except for micro and small enterprises. Therefore, Luxembourg would like to suggest to add "all" to the Art2.1. The current wording could lead to diverging interpretions.

Art2.2.(b): With reference to the point 23 in article 4, more specifications are needed in the text or in the annexe explaining the objective for including public administrations in the scope of the proposal NIS 2.0. The European Commission could further elaborate on what kind of public administrations are targeted here.

[1] Definition from Cybersecurity Act:
- 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;
- 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

Art2.2 last paragraph: The list of entities identified for public administrations and critical entities can contain sensitive information. Therefore, this paragraph could state that the list could be transferred to the European Commission in an anonymised way, meaning only the number per type of entity would be transferred, like it is currently the case for OES.

POLAND

Poland has a scrutiny reservation on art. 1 and 2 NIS2 as they are currently under examination.

Article 1 Subject matter

The wording of Article 1 should be discussed at the end of the negotiations as its provisions have to reflect the final content of the directive.

Article 2 Scope

1) **Para 1** – The issue of recognising the entities falling within the scope of the directive raises many questions and concerns.

There is a need to thoroughly discuss the size-cap rule and the practical consequences of this approach. The concerns of the CA should be addressed. With the size-cap rule approach it is crucial to design clear provisions accompanied by recitals. There should be no doubts, while reading the directive, which entities fall under its scope. In this respect there is a need for clarification. When having high penalties it is also crucial to establish the date from which the entity is obliged to fulfil the obligations.

Using the size-cap rule means that competent authorities may not know which entities fall under the scope of the directive, as in many sectors there are no registries of the entities of types referred to in the annexes, and in some cases, where there is a registry, there is no information about the size of the entity. The implementation should not imply the necessity to implement such registries and the draft should establish a common framework on how the CA could identify the entities falling under the scope of the directive.

Questions:

a) Could the EC confirm that the competent authorities will not have an obligation to identify individually the entities under their supervision? This seems to be implied by the current wording.
b) Should the entities self-report to the CA? A solution might be to foresee an obligation for the entities to indicate contact persons to the CA, by this the CA will know that an entity considers to be under the scope of NIS2.
c) What will be the date from which the entity is obliged to implement all the obligations foreseen in the NIS2?
d) What will be the consequences if during a year the entity will not employ all the time minimum 50 people (for example in some months under 50, and some below)?

2) **Para 2.a.ii** – regarding the trust service providers

There is a need for thorough analysis of the necessary changes to eIDAS following the inclusion of TSPs to the NIS. The deletion of art. 19 of eIDAS seems not to be sufficient. It should be noted that „supervisory body" from eIDAS is not the same as „competent authority" from NIS2. Different scenarios could emerge and there should be clarity on that.

Would there be two authorities, one being the CA (for measures in art. 18 NIS2) and the other the supervisory body (for ex ante supervision of qualified TSPs - article 24 eIDAS and ex post supervision of non-qualified TSPs)? Could supervisory body be also the CA? The relations should be clear to avoid any conflict of competences.

Another question would be the designation of both qualified and non-qualified TSPs as operators of essential services, regardless of their size. This represents a different approach in the supervision of non-qualified TSPs, given that under eIDAS regulation they are subject to a light-touch ex-post regulation. The NIS2 proposal implies that the authority will supervise the security obligations of non-Q TSPs ex-ante, which may have an important impact for these companies (a number of them are small and micro enterprises and this might represent a disproportionate burden) and also for the supervisory body. We would like to hear more about the rationale behind this switch of approach for non-Q TSPs and know if the Commission has assessed the specific impact in the trust services sector?

There is also a need to analyse the reporting obligations. Under NIS2 (art. 4(5)) the definition of incident seems not entail the infringement of other eIDAS requirements for qualified TSPs, qualified signature or seal creation devices.

Another issue is the cross border cooperation. What would be the relations of SPOCs (art. 8 NIS2) to art. 18 eIDAS (mutual assistance of supervisory bodies)

There is also a formal issue. If NIS2 deletes art. 19 eIDAS, in the NIS2 implementation period, there will be no legislation in the scope covered by art. 19 eIDAS. There will be a legal loophole.

The NIS2 negotiations should take into consideration the results of eIDAS review, to be presented in the following months.

We would strongly encourage the EC to present a working document explaining all the concerns, including presented above, on the consequences of including the TSPs to NIS2. This should also be discussed with experts in the art. 19 eIDAS group.

3) **Para 2.a.i** – There is also need for thorough analysis concerning the deletion of art. 41 and 41 of directive 2018/1972. We would also encourage the EC to present a working document on that. The new framework should take into account the best practises and experience gathered in the telecommunication sector. For example it is necessary to clarify if ENISA will still publish the recommendations on technical measures.
4) **Para 2.b** Poland will have comments to definition of public administration to adjust it to Polish legal system
5) **Para 2.c** In article 2 there is no requirement that the service depends on network and communications system. It is foreseen, however, in article 18. Not including network and information systems in the scope of identifying essential services may lead to including entities, that do not have any IT systems in the scope of the directive. Also, it can lead to different interpretations of the term "sole provider of a service". Did the EC consider that?
6) **Para 2.f** – the wording is quite vague. Could the EC elaborate on what kind of entities are to be concerned?
7) **Para 2 last sentence** – list of entities. What were the EC thoughts how should MS identify the entities pursuant to point b) to f). Should it be made like OESs under NIS1 – individual identification? Could MS foresee additional conditions for identification?

Questions and comments concerning the list:

a) What is the purpose of creating a list of entities identified pursuant to point b) to f)? Why the EC needs to gather this information?
b) Will the list be public? Who will have the access to the information send by the MS? The rules of access are of crucial importance considering that the list may entail sensitive information.

c) The list should be updated every time a new entity is identified, that should be a constant process. The deadline of two years seems not to be appropriate, it should be done when necessary.

The deadline is too short, it should be at least 12 months.

8) Para 6

Lex specialis rule is one of crucial issues to discuss. The approach to sectoral legislation should be same. The draft currently takes two different approaches, on the one side the deletion of article 19 e-IDAS and art. 40-41 EEC and inclusion of the entities, on the other the exemption of DORA entities.

Poland strongly believes that NIS2 should be considered as a horizontal legislation establishing the cybersecurity framework for all sectors that are covered, including the set of basic cybersecurity requirements. This framework, including requirements, can be further developed with sector specific regulation, but should not be changed in principle. It is essential to avoid fragmentation and silo approach, as this implies lack of situational awareness and weakening of the cybersecurity at the European level.

For Poland it is crucial to ensure that entities covered by sectoral legislation have an obligation of incident reporting to the CSIRT or competent authorities.

Therefore there is a need for changes to para 6 and Poland will propose such changes in the drafting process in close cooperation with other MS expressing similar views