Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 16 February 2021

WK 1627/2021 ADD 5

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 PL and SE

Delegations will find in Annex comments by PL and SE on the above-mentioned subject.

TABLE OF CONTENT

POLAND

Poland has a scrutiny reservation on art. 3 and 4 of the NIS2 as they are currently under examination.

1) We are wondering why in the Art. 4.1.b the word "or" was omitted at the end of the phrase in letter b, in comparison from the definition in the NISD?

2) Art. 4.2

   a) The definition of 'security of network and information systems' is used in the text four times: in the definition of national strategy and in art. 18 and 22. However, in the definition of the national strategy, the term "security of network and information systems' was in one instance replaced by cybersecurity. Could the EC elaborate why this definition was left in the proposal, when the term of cybersecurity is introduced?

      Maybe we should use 'cybersecurity' concept consistently throughout the text as defined in Regulation (EU) 2019/881?

   b) We should discuss adding at the end of the definition the phrase: "or availability of those networks and information systems"

   c) If the TSPs are added to the scope, shouldn't we also add the term "non-repudiation" to the definition, which concerns the electronic signature?;

3) Art. 4.4 – why was the term "the security of network and information systems" not replaced by the term "cybersecurity";

4) Art. 4.5 – could the EC explain why were changes made to the definition of an incident in comparison to the one in NISD?

   Moreover, DORA introduces the definition of an "ICT-related incident' (meaning an unforeseen identified occurrence in the network and information systems, whether resulting from malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, store or transmit, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity) and 'major ICT-related incident' (meaning an ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity). Could the EC elaborate why there is a need to introduce to the legal system these new definitions and not to align the definitions of NIS2 and DORA?

5) Art. 4.6 Why the actions like "identification, protection, detection, responding and recovery" were not included in the definition of incident handling?

6) Art. 4.8 The term 'Asset' comes from a different set of concepts. We suggest to use 'information' and the wording could be: "a weakness, susceptibility or flaw of system, process or control that can be exploited by a cyber threat and can lead to loss of confidentiality, integrity or availability of information";

7) Art. 4.13 Could the EC elaborate why there was a need to change the definition of DNS, in comparison to the one in NISD?

8) Art. 4.14 Could the EC elaborate why there was a need to change the definition of DNS service provider, in comparison to the one in NISD? There should be a good reasoning to change definitions that are already used and are known by the stakeholders.

9) Art. 4.15 Could the EC elaborate why there was a need to change the definition of 'top–level domain name registry', in comparison to the one in NISD? There should be a good reasoning to change definitions that are already used and are known by the stakeholders.

10) There is no definition of risk in the NIS2, while there is one in the NISD. DORA introduces the definition of ICT risk ('ICT risk' means any reasonably identifiable circumstance in relation to the use of network and information systems, - including a malfunction, capacity overrun, failure, disruption, impairment, misuse, loss or other type of malicious or non-malicious event - which, if materialised, may compromise the security of the network and information systems, of any technology-dependant tool or process, of the operation and process' running, or of the provision of services, thereby compromising the integrity or availability of data, software or any other component of ICT services and infrastructures, or causing a breach of confidentiality, a damage to physical ICT infrastructure or other adverse effects). Could the EC elaborate why the definition of the risk was not included and why there is a need to have a new definition of ICT risk in the legal system?

11) Art. 4.17 there is a mistake in the definition of "online marketplace' - a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council; There in no point (n) in art. 2 of Directive 2005/29/EC.

12) Art. 4.19 could the EC elaborate why there is a need to change the definition of the 'cloud computing service'?

13) Art. 4.22 the NIS2 has a definition of 'social networking services platform', while the DMA has the definition of "online social networking service" - means a platform that enables end users to connect, share, discover and communicate with each other across multiple devices and, in particular, via chats, posts, videos and recommendations. There should be one definition in the legal system when regulating the same thing. Therefore we see a need for changes in the NIS2 or the DMA. Could the EC comment if there is a need to have these two definitions? Moreover, what should be taken into consideration is the definition of an online platform in the DSA?

14) Art. 4.23 'public administration entity'

   a) Do we understand correctly that the entity must fulfill all four requirements (points a,b,c and d)?

   b) Why the requirement to have a legal personality was included in the definition? In Poland the public entities of the State Treasure (like for example the Chancellery of the Prime Minister, the ministries, agencies) do not have their own legal personality but they all act within the legal personality of the State Treasury (so called stationes fisci of the State Treasury) In practice this means that the entities responsible for the most important public registries would not be considered public entities under the NIS2, while smaller ones, from the regions, could. In the Polish case almost none of entities of the central government would fall under the scope of NIS2.

c) Could the EC elaborate why only the entities of NUTS level 1 and 2 were chosen? Most of mayor cities are excluded.

d) Could the EC give examples of "powers to address to the natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital"?

e) How does the EC see the process of identifing the public administration entities? As there are four additional requirements in the definition, it is not possible to simply use the size-cap rule. If an entity is of a kind defined in Annex 1, there would be a need to check if other criteria from the definition are met.

f) If an entity carries out activities in the area of public security, law enforcement, defence or national security, but these activities are not the main ones, would it mean that these entities are excluded from the scope?

g) Could the EC give examples of the entities meeting the criteria from point c?

SWEDEN

Article 3

It is positive that Member States may adopt or maintain provisions ensuring a higher level of cybersecurity in national legislation. As previously pointed out it is of utmost importance that the Directive does not prevent Member States from taking necessary measures to protect national security, as this in all circumstances falls under Member States exclusive competence. This means among other things that the Member States have the right to deviate from the Directive for the purpose of protecting the national security. It is also necessary to ensure that the proposed Directive in part does not interfere with issues that should be regulated on a national level. Considering the fact that the scope of the Directive is so far-reaching, SE is hesitant regarding minimum harmonization at the specified level.

SE would also like the Commission to clarify what applies if there is a corresponding provision in national legislation – does it mean that the entity does not need to apply the Directive at all?

Article 4

4 (2) and 4 (5)

Regarding the wording "any *action* that compromises" – SE would like to urge caution about this wording so that the Directive is not unintentionally limited to antagonistic threats.

Furthermore, regarding Article 4 (2) - SE would like to emphasize some challenges in transferring electronic communications from Directive of establishing the European Electronic Communication Code (EU 2018/1972) to NIS2.

In the EECC the definition of security is:

> *'security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of* ***those networks and services****, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;*

While the definition of security in NIS2 is:

> *'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;*

NIS2 only aims at availability/authenticity/accuracy/confidentiality in stored/transmitted/processed data and in the services offered or made available via the network and information systems. The EECC on the other hand, also aims at the security of the electronic communications networks and services themselves. If NIS2 is to be applicable to the electronic communication sector, the definition needs to be in line with the definition in the EECC.

Sweden sees the same challenge in regards to the definition of *incident* in NIS2, which also needs to be adjusted so that incidents include events that affect the communication networks and services themselves and not just other services etc that are offered by, or accessible via, such networks.

SE asks the Commission to clarify how the NIS2 should be applied to electronic communications networks and services, which are not quite comparable to other essential services since they constitute the foundation upon which all other network and information systems rely. How does the Commission view the fact that the definitions of security and incident are not as comprehensive in NIS2 as in the EECC?

4 (14)
SE would like the Commission to elaborate about DNS service provider and to clarify the meaning of *"entity that provides recursive or authoritative domain name resolution services"*? Is the purpose of this paragraph to cover all root servers?

4 (15)

SE would like the Commission to clarify what does it mean that an entity "*has been delegated"*?

4 (17)

Regarding "*online marketplace*" and the reference to Article 2 point (n) of Directive 2005/29/EC, SE notes that there is no such point in that Directive, Article 2 only has points from A-L. Is the reference incorrect?

4 (23) and 4 (24)

SE would like a clarification regarding Articles 4(23) and 4(24).

In the definition in Article 4(23) it is stated that the public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded. Does that mean that the Directive will not be applicable on an entity which is partly engaged in such activities at all or only in part? For example, a large part of the Swedish authorities has activities that are important for the total defence and Swedish security in general. This should be clarified in Article 4(23).

Furthermore, there are also many private actors active in total defence and national security which are covered by the definition in article 4(24). They should consequently be excluded from the scope of the Directive. There is however no exception for such activities in paragraph 24. This should be clarified in article 4(24).

4 (25) and 4 (26)

SE would like the Commission to elaborate on the need to differentiate between important and essential entities.

SE would also like the Commission to further define the concept of risk and the meaning of disruption since it is of great importance that the Member States have a common interpretation of such a central concept.