Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 26 April 2021

WK 5420/2021 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 and questions on Recitals by EL and PL delegations

Delegations will find in Annex comments and questions on Recitals by EL and PL delegations.

TABLE OF CONTENT

GREECE

- (9):" *Member States should be responsible for establishing a list of such entities, and submit it to the Commission"*
  We reiterate that instead of the submission of a list of entities to the Commission, 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*"

- (47): The criteria defined in this recital should be omitted. Such criteria could be discussed and decided within the Cooperation Group.

- (54): "*The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. "*

  a. In the aforementioned statement of recital 54, we suggest the inclusion of a specific reference to the respect of the protection of the fundamental rights of individuals and especially the right to privacy
  b. We agree with the recommendation made by the EDPS (see Opinion 5/2021, point 64) for a clarification that this recital should not be construed as an endorsement of weakening end – to -end encryption through "backdoors" or other similar solutions.

- (59): We suggest the incorporation of a clarification that the conditions of lawful access should be further specified under national legislation.

- (63), (64): While it is clearly stated that the entities concerned fall under the jurisdiction of the main establishment, we consider that clarifications are needed as per the applicable national provisions (especially implementing art. 18 and 20) under which other establishments of these providers shall be subject to. Such clarification might be included in a separate recital.

- (71), (72), (73), (75), (76):

  - A clarification is needed regarding the liability of top management positions and legal representatives in relation to public administration authorities. An explicit reference that the determination of the specific positions shall be performed by national legislation would be highly beneficial in this direction.
  -A clarification could also be included regarding the imposition of administrative fines -and sanctions in general- when the entity provides services in two or more Member States.

- (79): "*A peer-review mechanism should be introduced, allowing the **assessment** by experts designated by the Member states of the implementation of cybersecurity policies, **including the level of Member States' capabilities and available sources**".*

  We reiterate our reservations regarding the implementation of a peer review mechanism for the implementation of this Directive. Such reviews could be performed only on a voluntary basis. An alternative could be a mechanism to facilitate technical assistance.

- (80): "…*the power to adopt acts in accordance with article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes."*

  More details and clarifications as regards the consistency of the NIS 2.0 framework with the framework of the Cybersecurity Act, should be included, given the fact that delegated acts under 290 TFEU are non-legislative acts.

POLAND

1) Recital 11 – states that penalty regimes between essential and important entities should be differentiated but art. 31 does not introduce such differentation.
2) Recital 12 – PL believes that this recital needs redrafting to ensure that **the NIS2 is the main horizontal legislation**, and sector-specific legislation cannot change the cybersecurity framework established in the NIS2, especially the incident notification.
3) Recital 13 - the wording of this recital should be aligned with the changes made to the DORA proposal.
4) Recital 23 – PL believes that incidents concerning financial sector entities should be notified directly to CSIRTs. The CSIRTs should be always directly engaged in the process of incident handling. The SPOCs should not be intermediaries in this respect. NIS2 and DORA should not establish different regimes for incident reporting and handling.
5) Recital 25 – what is the aim of including the part on GDPR?
6) Recital 28 and 29 – the provision on coordinated vulnerability disclosure needs clarification to be in line with what is written in the recitals. The tasks of the CSIRT coordinator should be in articles.
7) Recital 31 – could the EC elaborate what would be the structured cooperation agreements? What is meant by this?
8) Recital 34 – states that the CG should organize regular joint meetings with relevant private stakeholders from across Union. Could the EC elaborate how this should work in practice, how the stakeholders will be chosen and if this is not a duplication with the works of the Competence Centre or activities of ENISA?
9) Recital 35 – states that the CAs should take the necesssary measures to enable officials from other MS to play an effective role in the activities of the host CA. Could the EC explain what is meant by this? What role could the visiting CAs have?
10) Recital 37 – it should be stressed that CyCLONe is only for large scale incidents and cyber-crisis and the rules of procedure concern only such cases. There should not be duplication or overlaping with the CSIRT Network and the NIS CG.
11) Recital 38 and 39 – definitions should be in article 4.
12) Recital 46 – states that the CG should carry out the sectoral coordinated supply chain analysis, whereas art. 19 states that the CG may carry out such analysis. This needs adjusting.
13) Recital 55 – states that MS should ensure that the requirement to submit initial notification does not divert the reporting entity's resources from activities related to the incident handling that should be prioritised. Could the EC explain how in practise this should be implemented by MS?
14) Recital 56 – We encourage the EC to present a working document how the idea of a single entry point could be implemented in practise to be in line with all the regulations.
15) Recital 57 – it is an obligation to report criminal activities to the law enforcement authorities therefore the wording of the recital should be adjusted as currently it states that MS should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement.

16) Recital 69 – states that the processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services **should constitute a legitimate interest** of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.
According to recital 47 of GDPR - given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, the legitimate interest as a legal basis **should not apply to the processing by public authorities in the performance of their tasks**.
Recital 69 NIS2 seems not to be in line with recital 47 GDPR. Could the EC elaborate on that.

17) Recital 70 – states that important entities should not document systematically compliance with cybersecurity risk management requirements. This idea seems not to be reflected in the articles of the Directive. Could The EC elaborate on that?