Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 23 April 2021

WK 5420/2021 ADD 1

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 FR, DE and HU delegations

Delegations will find in Annex comments and questions on Recitals by FR, DE and HU delegations.

TABLE OF CONTENT

FRANCE

Dans la perspective de la réunion du groupe horizontal sur les questions cyber du 28 avril 2021, les autorités françaises souhaitent partager avec la Présidence des premiers éléments d'analyse sur la proposition de directive en objet. Les autorités françaises tiennent cependant à souligner que l'analyse du document à l'échelle nationale se poursuit et que ces éléments pourraient être appelés à évoluer au cours des négociations.

Les autorités françaises souhaitent à titre liminaire**,** faire part de leur étonnement quant au niveau de détails de nombreux considérants. En effet, les précisions qui y sont inscrites semblent pour relever de dispositions. En outre, certains éléments des considérants pourraient avoir des impacts dimensionnant dans les choix organisationnels de certains Etats membres et souhaitent à ce titre appeler à la vigilance du Conseil et de la Commission européenne.

Au **considérant 24**, les autorités françaises souhaitent obtenir des précisions sur l'intention de la Commission concernant la notion de « séparation fonctionnelle » entre les tâches opérationnelles des équipes de réponse aux incidents de sécurité informatique (CSIRT) et les activités de surveillance évoquées dans ce considérant. En effet, afin de garantir cette séparation fonctionnelle, plusieurs lectures peuvent être adoptées : envisage-t-on ici une simple distinction des unités en charge de ces fonctions au sein de l'autorité nationale, et ce, même s'il revient à la plus haute instance décisionnaire de l'autorité nationale d'entériner les orientations prises ?

Au **considérant 31**, les autorités françaises s'interrogent sur la portée de la dernière phrase de ce paragraphe : "To avoid duplication of efforts and seek complementarity to the extent possible*, ENISA should explore the possibility of entering* ***into structured cooperation agreements*** *with similar registries in third country jurisdiction*". Cet élément, ne figure pas à l'article 6 auquel il est attaché et laisserait penser que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) aurait la capacité de conclure des accords avec des pays tiers.

Au **considérant 35**, les autorités françaises :

- soulignent que les dispositions évoquées dans ce considérant, outre le fait d'être trop prescriptives, relèvent, d'une part, d'une décision des Etats membres *in fine,* et d'autre part, d'arrangements administratifs entre États membres ;
- reconnaissent, en revanche, que dans la perspective d'un objectif de coopération loyale, il serait préférable d'inciter les États membres à aller en ce sens ;
- rappellent que certaines données échangées peuvent relever de la confidentialité et, qu'à ce titre, il conviendrait d'inclure une réserve à l'image du libellé retenu au considérant 66.

Au **considérant 36**, les autorités françaises :

- interrogent la Commission sur le type d'activités auxquelles pourraient participer des États tiers ou organisations internationales avec le Groupe de coopération et le *CSIRT network*, et qui nécessiteraient de recourir à des accords relevant de l'article 218 TFUE. L'avis des groupes visés sera indispensable à cet égard ;
- rappellent que les mesures prévues dans ce considérant ne figurent pas dans les articles 12 et 13, alors même que leur portée semblent davantage relever du corps des dispositions.

Au **considérant 44**, les autorités françaises accueillent favorablement la prise en compte des "*managed security services*" au sein de la directive. Comme mentionné lors de l'analyse de l'article 4, les autorités françaises considèrent que ce secteur gagnerait à être mieux pris en compte du fait de l'importance qu'il représente dans l'économie européenne. Ainsi, et pour permettre à la directive d'être à l'épreuve du futur, celle-ci gagnerait en clarté en définissant plus précisément ces entités, afin d'une part, de les identifier plus distinctement au sein du périmètre de la directive, d'autre part, de mieux encadrer la lecture de l'article 18.

Au **considérant 69**, les autorités françaises rappellent que les informations gérées par les autorités nationales et les CSIRTs relèvent du domaine de la sécurité et défense nationale.

Au **considérant 70**, les autorités françaises :

- souhaitent comprendre l'intention de la Commission sur la dernière partie de ce considérant : "*For the latter, this means that important entities* ***should not document systematically compliance with cybersecurity risk management requirements****, while competent authorities should implement* ***a reactive ex-post approach*** *to supervision and, hence, not have a general obligation to supervise those entities*". La lecture de ce considérant pourrait laisser entendre que les opérateurs importants n'ont pas à se conformer aux obligations de l'article 18 ;
- interrogent la Commission sur la signification d'une *"reactive ex post approach"* et sur la façon de la mettre en œuvre.

Les autorités françaises se tiennent à la disposition de la Présidence pour toute précision utile.

GERMANY

Please note: The following list of comments and questions regarding NIS2 Recitals is non-exhaustive and may be expanded in future discussions. Comments and questions are sorted by order of the Recitals.

1. Comment regarding Recital (8) – As already stated in the context of Art. 2, Germany believes that the size cap-rule as currently drafted leads to a significant increase of the number of entities in scope of NIS2, which in turn is detrimental to quality of supervision and leads to massive cost increases for the economy. With regard to the food-sector (i.e. the currently used definition thereof and the resulting great number of entities covered), this becomes particularly apparent. The size cap-rule as the only deciding factor is not apt to reflect the risk based approach intended with NIS2. In our view, the criticality of supply of an entity needs to be taken into account.

2. Comment regarding Recital (9) sentence 2 – We would like to repeat our serious doubts regarding the creation and storage of a list of entities at a central point at the European level. We believe that such a list would be an attractive target for malicious state and non-state actors. Once such a list would fall into the wrong hands, we could not turn back time. European and national security interests would face significant danger from that point on. On the other hand, the Commission has – in our view – not shown a use-case for such a list that would justify the aforementioned risks.

3. Question regarding Recital (12) sentence 2 – The empowerment to issue guidelines ("in relation to the implementation of the lex specialis") does not appear to be included in the articles. We would appreciate a clarification by the Commission in this regard.

4. Question regarding Recital (16) – The definitions of scalable, elastic and shareable are welcomed. The reference to ISO 17788:2014 in conjunction with the definition of "scalable" and "rapidly" results in our view that cloud providers currently covered who only offer vServers would no longer be covered. This is a deterioration of the current situation. It is desirable that vServer providers remain covered. Does the Commission agree that this should be remedied by an "or" link between the above-mentioned criteria?

5. Question regarding Recital (16) – Why has the Commission chosen to include "private cloud" as deployment model? Would that not lead to the inclusion of any entity that is running its own data centre?

6. Question regarding Recital (23) – Could the Commission kindly elaborate a bit further on the conditions for forwarding incident notifications? What is intended by the term "affected"?

7. Question regarding Recital (25) – Could the Commission kindly explain if "proactive scanning" is to be understood as pen-testing for vulnerabilities or testing with regard to compromised systems? Could the Commission kindly elaborate on the appropriate legal basis in data protection law? We would also like to note a possible editorial error in the recital as it states "as regards personal data" twice.

8. Question regarding Recital (34) – Could the Commission kindly explain why it saw the need to prescribe "regular joint meetings with relevant private stakeholders" and not leave it up to the organizational autonomy of the Cooperation Group? What benefit does the Commission see in such meetings?

9. Question regarding Recital (37) – Why has the Commission chosen not to involve the Cooperation Group or the CSIRT-Network in the decision making process of cooperation / participation with third countries (as currently done with the UK)? Why is the word "should" used in sentence 2 instead of "must" or "shall" with regard to protection of data?

10. [Comment regarding Recital (39) – "Near misses" are in our view rather difficult to operationalize and we are not convinced that the phenomenon suitable to be legally defined.

11. Question regarding Recital (55) – The recital mentions a "two-stage approach", while the incident reporting provision actually includes three stages. We would appreciate a comment by the Commission in this regard.

12. Question regarding Recital (56) – Why are the data protection supervisory authorities not directly involved in the creation of a "notification template"? After all, the template should also cover the information to be provided in accordance with article 33 para. 3 GDPR.

13. Question regarding Recital (57) sentence 2 – The sentence's meaning is unclear. In the Commissions view, how should the facilitation of coordination between the competent authorities look like in concrete terms and to what extent exchange of personal data goes alongside such facilitation? Why is data protection only mentioned in relation to Europol? In our view, a general reference to the applicable data protection legislation, covering all actors involved, would be preferable.

14. Comment regarding Recital (59) – We welcome the fact that Rec. 59 refers to compliance with data protection law. However, we would like to reiterate the importance of also specifying the WHOIS-data to be stored by registrars. This creates legal certainty for registrars and ensures uniform implementation across the Union.

15. Question regarding recital (62) – In our view, it should be ensured that claimants are not burdened with disproportionate costs when they are lawfully asserting their claims. Does the Commission approve and is an addition to the recital or Art. 23 preferable?

16. Question regarding Recital (69) – The first sentence seems to refer to Article 6 para. 1 subpara. 1 point (f) GDPR, which is deemed to form a legal basis for processing personal data for the purposes mentioned in this recital. However, persuant to Article 6 para. 1 subpara. 2, said provision is not applicable to the processing of personal data by public authorities. Does the Commission agree that insofar, the recital needs to be amended? Moreover, it is not entirely clear whether Article 6 para 1 subpara 1 point (f) of the GDPR can in any case serve as legal basis, since the application of said provision requires a balancing exercise, i.e. also taking into acccount the interests of the data subject („*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject*"), and in particular where the data subject is a child. A more general reference to the GDPR without being to specific about the exact legal basis for data processing could be preferable.

17. Question regarding Recital (72) – According to Art. 33 Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary. This is not limited to administrative fines. Could the Commission elaborate, why in Recital 72 only administrative fines are referred to?

18. Question regarding Recital (73) – We kindly ask the Commission to explain why recital 73 uses the term "undertaking in accordance with Articles 101 and 102 TFEU"? In other Union regulations, the term "legal person" is used, as e.g. in Art. 60 para 5 of the Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Remark regarding Recitals (73 to 75) – In our view the structure of Recitals 73 to 75 does not follow the system of Art. 31 to Art. 33 of the Directive, since the Recitals include statements for fines on essential and important entities as well as to natural persons. We recommend restructuring the Recitals in a clearer order.

HUNGARY

General comment:

We would like to note that some recitals do not elaborate on important articles in sufficient detail.

Recital 7 and 8

We would like to repeat our previous comment, namely that the size of entities should not be the only threshold used. In the essential sectors and subsectors, the scope of NIS2 should cover entities that provide an essential service in a Member States. We therefore consider it necessary to maintain national identification based on thresholds that express the entity's significance within a sector or sub-sector.

Recital 10

We would like to know how the **Commission's guideline in recital 10** would fit into the tasks of the Cooperation Group (CG) under Article 12. The CG can provide guidance on the transposition and implementation of this Directive, in accordance with Article 12 paragraph 4. (a). Why did the Commission consider it necessary to treat one aspect of the transposition of NIS2, namely the national identification of micro and small enterprises, separately and not to facilitate its uniform application by means of guidance issued by CG?

Recital 16

Also, why did the Commission find it necessary to include such detailed rules on **cloud computing services in recital 16**?

Recital 38 and 39

Furthermore, we would like know why certain definitions, such as **risk in recital 38** and **near-misses in recital 39** are included in the recitals and not in Article 4. Similarly, why are the criteria to be considered when **imposing fines on "persons that are not an undertaking**" is listed in **recital 73** instead of Article 29?

DORA related recitals (13 and 23)

Regarding **recital 13**, we were glad to see that the new compromise proposal of DORA extends the reporting obligation to significant threats.

DORA authorities will be required to provide details of reported incidents to NIS SPOCs **(recital 23**). However, the NIS2 articles on information do not apply to the financial sector according to the recitals. Taking into account that information on incidents and threats concerning the financial sector are necessary to form a complete picture of the state of the European cyberspace, we are interested in how DORA-related information will be incorporated in monthly SPOC reports [Article 20 (9)] and the work of the CSIRT network.

Overall, it would be very helpful if the Commission could precisely indicate the articles of NIS2 that would remain applicable to the financial sector. We would also welcome more information on how information concerning entities in the scope of NIS2 but reported under will under DORA and transmitted to the NIS SPOC would be incorporated into the NIS2 information sharing and cooperation mechanisms.

Recital 51

The elements of public electronic communications networks mentioned in recital 51 are especially vulnerable to attacks aimed at mass data collection. Therefore, we will suggest mentioning encryption as a concrete example of cybersecurity measures.

Recital 56

Furthermore, we ask the Commission to elaborate on its idea to create a **„single entry point" in recital 56** and explain how it will fall in line with the operative articles, especially Article 32.