



Council of the European Union
General Secretariat

**Interinstitutional files:
2020/0359(COD)**

Brussels, 19 April 2021

WK 5081/2021 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 by FR and LT delegations on Articles 35-43

Delegations will find in Annex comments by FR and LT delegations on Articles 35-43.

TABLE OF CONTENT

	Page
FRANCE	2
LITHUANIA	4



FRANCE

Dans la perspective de la réunion du groupe horizontal sur les questions cyber (GHQC) du 19 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, obtenir des précisions sur l'intention de la Commission européenne 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 au considérant 24 : cette disposition pourrait avoir un impact significatif sur certains modèles de gouvernance nationale.

Sur l'**article 39**, les autorités françaises rappellent leur position évoquée au GHQC du 9 février, concernant la suppression de l'article 19 du règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS) :

- les autorités françaises remercient la Commission pour ses premiers éclairages sur ce volet et ont bien pris note de son analyse selon laquelle il n'existait pas de risque de duplication, puisque les dispositions seraient transférées vers la directive NIS2, soumettant ainsi les fournisseurs de services qualifiés et non qualifiés au cadre de notification tel que prévu par l'actuelle directive NIS (supervision *ex ante* en l'occurrence) ;
- toutefois, les autorités françaises souhaitent attirer l'attention des États membres et de la Commission sur certains enjeux :
 - la migration des exigences d'un règlement vers une directive contrevient à l'objectif d'harmonisation poursuivi par le règlement eIDAS, puisque les transpositions nationales pourraient différer et ne pas intervenir dans le même temps ;
 - les champs de la directive NIS et du règlement eIDAS ne sont pas les mêmes : les contrôles prévus par les autorités de supervision au sein du règlement eIDAS relatifs aux prestataires de services de confiance sont entendus largement (par exemple, l'identification des utilisateurs, la procédure de délivrance de *tokens* physiques), contrairement à la directive NIS, qui limite ces contrôles aux réseaux et systèmes d'information ;
 - par ailleurs, l'obligation de notification d'incident ne vise pas les mêmes incidents du fait des périmètres différents entre les deux actes européens ;
 - l'article 19 du règlement eIDAS renvoie également à d'autres articles du règlement eIDAS applicables aux prestataires de services de confiance (PSCo), dont les articles 13, 20, 21, 24 et 31. Or, la directive NIS ne comporte aucune exigence relative à ces articles ;
 - ainsi, les autorités françaises appellent à la vigilance pour que la révision de la directive NIS n'abaisse pas le niveau de sécurité prévu au titre du règlement eIDAS.

Sur l'**article 40**, les autorités françaises rappellent leur position évoquée au GHQC du 9 février, concernant la suppression des articles 40 et 41 de la directive (UE) 2018/1972 (Code européen des communications électroniques) et :

- expriment leur inquiétude quant au risque de régression en matière d'obligations de sécurité des entreprises des communications électroniques en cas de suppression des 40 et 41 du Code européen des communications électroniques (CECE) au regard, d'une part, de la différence de périmètre couvert par les deux textes : NIS relevant uniquement de la cybersécurité alors que le CECE traite de la sécurité dans son entièreté (par exemple, les pannes, incendies, incidents climatiques etc.) et, d'autre part, au regard du manque d'alignement des définitions entre les deux textes. En effet, la formulation retenue dans la proposition de directive NIS2 sur les « réseaux et systèmes d'information » pourrait laisser à penser que les « services de communications électroniques », définis dans le CECE, sont exclus de ces dispositions ;
- expriment leur souhait, en l'état actuel de la proposition de directive, de maintenir les articles 40 et 41, afin de conserver le principe général de responsabilité des opérateurs dans la sécurisation de leurs réseaux et services ;
- rappellent le besoin de proportionnalité dans les obligations de sécurité demandées aux opérateurs, en fonction de leur taille puisque, contrairement à la majorité des secteurs soumis à NIS2, les TPE et PME du secteur des communications électroniques ne seront pas exclues du champ d'application.

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

LITHUANIA

Disclaimer:

The following questions in relation to Articles 35-43 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.

Points of clarification:

Article 35:

With a view of recently established European cyber crises liaison organisation network (EU – CyCLONe), as indicated in Article 14 in the Proposal, would it not be relevant to add its reports in addition to the reports of the Cooperation Group and the CSIRTs Network on the experience gained at a strategic and operational level?

Article 35:

Could you elaborate on the proposal made to set the submission of the first report by the Commission on the functioning of this Directive 54 months after the date of entry into force of this Directive?

Article 38:

Given the significant changes brought by the Proposal we would like to ask to reconsider the suggested transposition period and prolong it from 18 months to 24 months.

Articles 39 and 40:

Could you elaborate the reasoning behind the rationale to delete the referred Articles? Has there been an analysis made of possible impact of the two repealed provisions?
