Council of the European Union

Brussels, 28 June 2021
(OR. en)

10236/21

Interinstitutional File: 2020/0359(COD)

CYBER 188
JAI 791
DATAPROTECT 179
TELECOM 277
MI 510
CSC 257
CSCI 96
CODEC 986

COVER NOTE

From:	Mr. Roberto Viola, Director General, Directorate General of Communication, Networks, Content and Technology), European Commission
date of receipt:	28 June 2021
To:	Mr. Nuno BRITO, Ambassador, Permanent Representatives Committee – Part II, Council of the European Union
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 2016/1148 - Summary of the feedback received on the adopted proposal

Delegations will find in the Annex a letter from Commission Director General R. Viola (Directorate-General for Communications networks, Content and Technology) summarising the feedback on the NIS2 proposal received through the Commission's 'Have your say' webpage, between 16 December 2020 and 21 March 2021.

E-MAIL

IM 006797 2021
28.06.2021

Ref. Ares(2021)4093435 - 23/06/2021

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

The Director-General

Brussels
CNECT.H.2/JB

EP ITRE Chair Mr Cristian-Silviu BUŞOI
cristiansilviu.busoi@europarl.europa.eu
European Parliament
Bât. Altiero Spinelli 11E102
Rue Wiertz 60
B-1047 Brussels

Ambassador Mr Nuno BRITO
reper@reper-portugal.be
European Council
Rue de la Loi 175
B-1048 Brussels

Subject: **NIS Directive Revision – Summary of the feedback received on the adopted proposal**

Dear Chair Buşoi, dear Ambassador Brito,

On 16 December 2020, the European Commission adopted a proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ("the NIS 2 proposal"). The revision of rules on the security of network and information systems also features in the EU's Cybersecurity Strategy for the Digital Decade and a proposal for a Directive on the resilience of critical entities, adopted on the same day.

As part of its Better Regulation Agenda, legislative proposals adopted by the European Commission and their accompanying impact assessments are open to public feedback at the same time as being put forward to the European Parliament and Council. This letter summarises the feedback received through the Commission's 'Have your say' webpage[1], between 16 December 2020 and 21 March 2021.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Legislative-framework-for-the-governance-of-common-European-data-spaces

1. Respondents

The Commission received 121 contributions from different types of stakeholders: business associations (42%), companies/business organisations (33%), others (10%), non-governmental organisations (6%), EU citizens (3%), public authorities (2,5%), non-EU citizens (almost 2 %), academic/research institutions (<1%), trade associations (<1%).
Of the 121 replies, 91 originated from within the European Union. The other replies came from the United States (50%), United Kingdom (23%), Japan (<7%) as well as from China, Canada, Switzerland, Thailand and Iran (respectively around 3% per country). Out of the 40 companies and business organisations that responded, over 50% were large, 17.5% were medium, 10% - small and 20% - micro enterprises.

2. Feedback

The feedback received includes general comments on the proposal, as well as specific comments on its main chapters. The most recurrent comments are summarised below.

- *General comments on the proposal*

The respondents emphasised the positive role of the current NIS Directive for setting the ground for network and information system security in the EU and generally recognised the need for a more up-to-date, harmonised and future-proof cybersecurity legal framework. Therefore, the new proposal has been overall very much welcome. The comments therefore concern targeted suggestions for improvements of the text rather than an opposition to the general direction of the proposal. A number of respondents advocate a greater harmonisation and an improvement of security levels across the EU, however without causing unnecessary burdens or costs to the affected providers, particularly to small and medium-sized enterprises (SMEs).

- *On the definitions and scope of the proposal*

In general, respondents support an enlargement of the scope of the NIS2 proposal with some indicating that enlarging the scope has to be done carefully, in order not to impose disproportionate burden and additional costs (in particular on SMEs and important entities). Some respondents suggest streamlining certain definitions in order to align with related Commission proposals (such as the Digital operational Resilience Act for the financial sector (DORA) and the Critical Entities Resilience Directive (CER).

- *On security measures and incident reporting obligations*

The feedback on security measures as provided in the NIS 2 proposal is generally positive. Respondents particularly praise the prominence given to risk-based approach to security measures. A recurring comment relates to the use of cybersecurity certification schemes and the relation with the Cybersecurity Act (Article 21 NIS2), as a number of participants see greater benefits in certification schemes of a voluntary nature. As regards incident reporting obligations, a number of respondents are in favour of aligning the current reporting deadlines with those under the GDPR. They are mostly concerned about the administrative burden on companies and the lack of overview on the significance of the incidents within the 24h timeframe. Moreover, there appears to be some uncertainty about the definition of significance in general and in connection with the reporting of "threats" in particular.

- *On supervision and enforcement*

Respondents support the further clarification of the provisions on supervision and enforcement. Some stakeholders also signalled some concerns with the level of fines under the NIS2 proposal.

- *On alignment with other related initiatives and EU legislation*

Last but not least, a large number of respondents appeal towards a consistent and coherent approach to related cybersecurity initiatives and legislation such as DORA and CER. A few replies generally welcome the attempt to bring the sector-specific security requirements for electronic communications services and networks into the horizontal NIS framework under the condition that does not cause any disruptions and unnecessary burden on companies.

Yours sincerely,

(Electronically signed)

Roberto Viola

c.c.: Bernardo Costa Pereira, Chair of the Horizontal Working Party Cyber in charge of the file
F. Comptour, (CAB Breton)
K. Szczucka, N.Vandystadt, T. Doise, L Boix Alonso; F. Vianello, J. Boratynski; B. Hristova-Ilieva