Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 18 May 2021

WK 6380/2021 ADD 1

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI
PROCIV

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
N° Cion doc.:	14150/20 [COM (2020) 823 final]
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: interaction with sectoral legislation - Additional comments by PL delegation

Delegations will find in Annex additional comments by PL delegation on the above-mentioned subject.

Polish position and comments

on the interaction of NIS 2 Directive with sectoral legislation

General position

Poland is in favour of strengthening the importance of the NIS2 Directive as the main horizontal legislation in the field of cybersecurity. We should provide safeguards that future sectoral legislation does not change the main principles of the NIS2 framework when it comes to cybersecurity requirements and incident notification. For PL it crucial that incident notifications from all sectors are sent directly to CSIRTs. The basis set of cybersecurity measures should be consistent throughout all sectors. The silo approach should be avoided as it leads to fragmentation and lack of common situational awareness.

Lex specialis rule

The clause used is art. 2.6 "at least equivalent" is unclear and would cause many difficulties in practice.

Drafting proposals marked in yellow:

Recital 12

Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. As a minimum baseline Sector–specific Union legal act should require essential or important entities to adopt cybersecurity risk management measures and to notify incidents or significant cyber threats in line with requirements laid down in Articles 18 (1-2) and Article 20 of this Directive. Where sector-specific legislations foresee specific rules on supervision and enforcement, these rules should apply. The Commission may issue guidelines in relation to the implementation of the *lex specialis*. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. *Nevertheless while adopting the additional sector-specific Union acts the need of a comprehensive ans consistent cybersecurity framework should be duly taken into account.* This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Art. 2.6

Where provisions of sector–specific acts of Union law require essential or important entities to adopt cybersecurity risk management measures and to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.

Art. 2.7

Sector-specific acts of Union law referred to in paragraph 6 should at minimum include:

(a) cybersecurity risk management measures as laid down in Article 18 (1) and (2); and

(b) requirements to notify incidents and significant cyber threats as laid down in Article 20 (1- 4)

Relation with the DORA

DORA negotiations seems to be more advanced and it is possible that will finish sooner that the NIS2. It should be clear which provisions from the NIS2 would apply to entities covered by DORA. Therefore, PL proposes to indicate precisely in the recital and in art. 2 of the NIS2 which provisions of the NIS2 would not apply to the entities under DORA.

Relation with eIDAS

PL strongly supports the deletion of art. 19 eIDAS and incorporation of the TSPs into the NIS2 framework. Nevertheless to fully encompass the scope of the changes needed in the provisions of the eIDAS and the NIS2, to make sure that the changes are consistent and preserve the undisturbed functioning of the system, it is essential to see the changes that will be proposed by the EC in the course of the eIDAS review.

PL would also strongly encourage the EC to present a working document explaining in details the impact of the TSPs incorporation to the NIS2 framework for the functioning of the eIDAS framework.

Currently what is needed is a provision stating that the deletion of the article 19 of the eIDAS enters into force at the day when the NIS2 implementation date expires. This is needed to avoid legal loophole during the time for the NIS2 implementation to national legislation, as the eIDAS is a regulation and the NIS2 a directive with a time prescribed for the implantation.

Therefore PL proposes the following addition in art. 42.

Art. 42. This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union, with exception to Article 39 which enters into force on the day following the day when the transposition deadline as laid down in Article 38 expires.

Relation with ECCC

PL strongly supports the deletion of articles 40 and 41 of the ECCC.