Council of the European Union
General Secretariat



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

**Brussels, 16 April 2021**

**WK 5081/2021 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<br>- Comments and questions by EL delegation on Articles 35-43 |

Delegations will find in Annex comments and questions by EL delegation on Articles 35-43.

**GREECE**

- Art. 36 (exercise of delegation):

- Pursuant to this article the Commission is empowered to adopt delegated acts in accordance with art. 290 TFEU.

- According to art. 21 (2) "The Commission shall be empowered to adopt **delegated acts specifying which categories of essential entities shall be required to obtain a certificate** and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36."

- In addition, the Cybersecurity Act (EU 2019/881) sets the rules for the establishment of a European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognized and used in all Member States. In particular, each European scheme should specify, inter alia, the categories of products and services covered and the cybersecurity requirements, such as standards or technical specifications (art. 54).

According to art. **56 (2)** of the Cybersecurity Act: "The cybersecurity certification shall be voluntary, unless otherwise specified by **Union law** or Member State law".

- However, **according to art. 290 (1) TFEU:** "A legislative act may delegate to the Commission the power to adopt **non-legislative acts** of general application to supplement or amend certain non-essential elements of the legislative act."

**Question – request for legal clarification**: How do we ensure consistency of the NIS 2.0 framework with the framework of the Cybersecurity Act, given the fact that delegated acts under 290 TFEU are non-legislative acts?

- Art. 38 (transposition)

*"Member states shall adopt and publish, by… (**18 months after the date of entry** into force of this Directive) …"*

The NIS 2.0 proposal sets out an enhanced framework with concrete obligations and an expanded scope of application. Many new sectors and entities have been incorporated in this enhanced framework and new national mechanisms should be established for ensuring compliance. Several Member States have already stressed out the need for more resources, regarding effective implementation of the new framework. Transposing the NIS 2 Directive into national legislation within an 18-month period might be unrealistic. Extension of the period of transposition may therefore be needed, especially after taking into account the discrepancies in Member State's capabilities and the estimated number of entities expected to comply with the requirements of NIS 2.0, in comparison with the existing entities under the scope of NIS 1.0.

Economic and structural impact on public administration and private sector should also be taken into account.