Council of the European Union

Brussels, 12 May 2023
(OR. en)

9060/23

LIMITE

CYBER 110
JAI 612
DATAPROTECT 137
MI 398
CSC 235
CSCI 75
CODEC 854
IA 105

Interinstitutional File:
2022/0272(COD)

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. prev. doc.:	14477/22, 12429/22 + ADD 1-6
Subject:	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102
	- Progress Report

The Presidency has drawn up a progress report on the proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, in order to report on the work carried out so far by the Council preparatory bodies and on the state of play in the examination of the proposal.

This report was presented by the Presidency to the Horizontal Working Party on Cyber Issues (HWPCI) at its meeting on 12 May 2023.

INTRODUCTION

1. On 15 September 2022, the Commission adopted the proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 ('Cyber Resilience Act'). First announced by President von der Leyen in her State of the Union Address in September 2021, the idea was reflected in the Council conclusions of 23 May 2022 on the development of the European Union's cyber posture, which called upon the Commission to propose common cybersecurity requirements for connected devices by the end of 2022. Prior to the announcement, the Council conclusions on the cybersecurity of connected devices of 2 December 2020 underlined the importance of assessing the need for horizontal legislation in the long term to address all relevant aspects of the cybersecurity of connected devices, such as availability, integrity and confidentiality, including specifying the necessary conditions for placement on the market.

2. The purpose of the proposal, which is based on Article 114 TFEU, is to harmonise essential cybersecurity requirements for products with digital elements in all Member States and avoid overlapping requirements stemming from different pieces of legislation. The proposal aims to fill the gaps in the existing cybersecurity legislation by ensuring that products with digital elements – for example Internet of Things (IoT) products, such as connected home cameras, refrigerators, TVs, toys and non-embedded software – become secure throughout the whole supply chain and throughout their whole life cycle. The proposal also aims to clarify links with existing legislation and to contribute to making it more coherent. Lastly, the proposal also allows users to take cybersecurity into account when selecting and using products with digital elements.

3. In particular, the proposal lays down:

    *   rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;

    *   essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;

- essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;

- rules on market surveillance and enforcement of the above-mentioned rules and requirements.

STATE OF PLAY OF WORK WITHIN THE COUNCIL PREPARATORY BODIES

4. Discussions on the proposal started in the Horizontal Working Party on Cyber Issues (HWPCI) on 21 September 2022 and a full read-through was completed on 26 October 2022. As a consequence of this read-though, Member States broadly welcomed the proposed Regulation and generally supported its overall objectives, albeit with some scrutiny reservations. Various topics such as the scope of the proposal, the product lifetime in conjunction with vulnerability handling requirements, the free movement clause, the interaction with other relevant legislation, the consequences for SMEs and start-ups and the reporting provisions needed further clarification and discussion. On 6 December 2022, the Council took note of the progress made under the Czech Presidency (14477/22).

5. The Swedish Presidency's priority was to advance the discussions as much as possible towards a general approach. In order to structure these discussions and allow delegations enough time for scrutiny, the Presidency circulated a detailed work schedule dividing the text into four major blocks of articles with a concrete timeline for their discussion. After an initial oral discussion of every single block, Member States were invited to submit written comments on that particular part, thus allowing the Presidency to draft a compromise text that would constitute the basis for the ensuing discussion. In accordance with this work schedule, four dedicated Working Party meetings took place on 18 January, 1 and 15 February and 1 March 2023. Based on the outcome of these discussions and Member States' comments, the Presidency prepared new compromise text proposals which were presented and discussed at the HWPCI meetings on 1, 15 and 29 March 2023.

6. The Swedish Presidency prepared a revised draft of the whole text of the proposal, which was discussed by the HWPCI on 26 April 2023. This new proposal has been broadly welcomed by Member States, although certain points still need to be further discussed, particularly the classification of products with digital elements with regards to their sensitivity (Article 6) and the related list (Annex III), the conformity assessment provisions (Article 24) and the reporting obligations (Article 11). Furthermore, Member States have expressed the need to establish clear and unambiguous provisions on dual-use products and software, including the status of open-source components and Software-as-a-Service. Member States have also raised concerns about the impact on SMEs and the lack of available harmonised standards for this Regulation.

7. The Swedish Presidency also organised workshops and thematic discussions on specific topics where Member States identified a need for further clarification and understanding. A first workshop was held on 9 March and concerned harmonised standards. On 20 April another workshop took place concerning vulnerability reporting and a thematic discussion was held on 3 May to address the reporting obligations in Article 11.

8. As a follow-up to the discussions under the Czech Presidency on the role and tasks which were envisaged for the European Union Agency for Cybersecurity (ENISA), on 15 February 2023 the Presidency invited the Executive Director of ENISA to exchange views with Member States on the role of the Agency under the CRA.

9. By the end of May 2023, the Swedish Presidency will have organised a total of ten HWPCI meetings on the Cyber Resilience Act.

10. The Presidency plans to continue these discussions in the coming weeks and remains keen to make sufficient progress to facilitate a general approach.

11. On the basis of the progress made under the Swedish Presidency, the incoming Spanish Presidency plans to continue the work on this important file.

12. In the light of the above, the Permanent Representatives Committee and the Council are invited to take note of the progress made on the examination of the proposal for a Regulation.