Council of the European Union

Brussels, 10 February 2023
(OR. en)

6305/23

Interinstitutional File: 2022/0272(COD)

LIMITE

CYBER 30
JAI 156
DATAPROTECT 39
MI 104
CSC 75
CSCI 23
IA 19
CODEC 174
TELECOM 38

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	5806/23, 5308/23
No. Cion doc.:	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: Articles 6, 18 - 24 and annex III - Presidency compromise proposal

Member States will find in Annex a Presidency compromise proposal on the provisions regarding the list of critical products (Article 6 & Annex III) and conformity assessment (Articles 18-24). This compromise proposal is based on the outcome of discussions during the HWPCI meeting on 1 February and written comments received from Member States. This proposal will be presented and discussed at the HWPCI meeting on 15 February 2023. Changes compared to the Commission proposal are indicated in **bold** and ~~strikethrough~~**.**

Article 6

Critical products with digital elements ***and highly critical products with digital elements***

1. **[**Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as ~~**falling in**~~ **belonging to** that category.**]**

   Categories of critical products with digital elements ~~**shall be**~~ **are** divided into class I and class II as set out in Annex III~~**, reflecting the level of cybersecurity risk related to these products.**~~ **The categories of products with digital elements listed in class I of Annex III meet one of the following criteria**:

   (a) the cybersecurity-related functionality of the product with digital elements, and in particular whether that product performs functions critical to security, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;

   (b) the product with digital elements performs a central system function, including network management, configuration control, virtualisation, processing of personal data, or functions having the potential to disrupt, control or damage a large number of other products with digital elements through direct manipulation.

   The categories of products with digital elements listed in class II of Annex III meet at least two of the following criteria:

   (a) the criteria referred to in the second subparagraph, point (a);

   (b) the criteria referred to in the second subparagraph, point (b);

   (c) the intended ~~**use**~~ **application of the product with digital elements** in sensitive environments[1], including in industrial **control** settings ~~**or**~~ **and** by ~~**essential**~~ entities of ~~**the**~~ **a** type referred to in ~~**the**~~ Annex **I** to ~~**the**~~ Directive **(EU) 2022/2555** ~~**[Directive XXX:XXXX (NIS2)]**~~**.**

2. **[**The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list **within each class** of **the** categories of critical products with digital elements a new category or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the ~~**following**~~ criteria **referred to in paragraph 1 of this Article** shall be taken into account~~**.:**~~

   ~~**(a) the cybersecurity-related functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:**~~

[1] Possible recital

~~(i) it is designed to run with elevated privilege or manage privileges;~~

~~(ii) it has direct or privileged access to networking or computing resources;~~

~~(iii) it is designed to control access to data or operational technology;~~

~~(iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection.~~

~~(b) the intended use in sensitive environments, including in industrial settings or by essential entities of the type referred to in the Annex [Annex I] to the Directive [Directive XXX/XXXX (NIS2)];~~

~~(c) the intended use of performing critical or sensitive functions, such as processing of personal data;~~

~~(d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;~~

~~(e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact.]~~

3. [The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by 12 months since the entry into force of this Regulation].]

4. Critical products with digital elements shall be subject to the conformity assessment procedures referred to in Article 24(2) and (3).

5. **[**The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate **at assurance level 'substantial' or 'high'** under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account **the criteria referred to in paragraph 1 of this Article** ~~**the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2,**~~ as well as ~~**in view of the assessment of whether that category of products is**~~ **any of the following criteria**:

(a) ~~**used or**~~ **the extent to which there is a critical dependency of entities of a type referred to in Annex I to** ~~**the**~~ **Directive (EU) 2022/2555 on the category of products with digital elements** ~~**relied upon byof the essential**~~ ~~**entities of a the type referred to in Annex [Annex I] to the Directive (EU) 2022/2555 [Directive XXX/ XXXX (NIS2)]**~~ ~~**or**~~ ~~**will have potential future significance for the activities of these entities; or**~~

(b) **~~relevant for the resilience of the overall~~ the extent to which cybersecurity incidents and exploited vulnerabilities concerning the category of products with digital elements can lead to** disruptive events[2] **for critical** supply chains ~~of products with digital elements against disruptive events~~ **across the internal market.]**

Article 18

Presumption of conformity

1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with the essential requirements covered by those standards or parts thereof, set out in Annex I.

2. Products with digital elements and processes put in place by the manufacturer, which are in conformity with the common specifications referred to in Article 19 shall be presumed to be in conformity with the essential requirements set out in Annex I, to the extent those common specifications cover those requirements.

3. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 and specified as per paragraph 4, shall be presumed to be in conformity with the essential requirements set out in Annex I **and related conformity assessment procedures** in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.

4. The Commission is empowered, by means of implementing acts, to specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I. Furthermore, **~~where applicable,~~** the Commission shall specify **~~if~~ for which assurance levels,** a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

[2] A recital may be added.

Article 19

[Common specifications][3]

Where harmonised standards referred to in Article 18 do not exist or where the Commission considers that the relevant harmonised standards are insufficient to satisfy the requirements of this Regulation or to comply with the standardisation request of the Commission, or where there are undue delays in the standardisation procedure or where the request for harmonised standards by the Commission has not been accepted by the European standardisation organisations, the Commission is empowered, by means of implementing acts, to adopt common specifications in respect of the essential requirements set out in Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Article 20

EU declaration of conformity

1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 10(7) and state that the fulfilment of the applicable essential requirements set out in Annex I has been demonstrated.

2. The EU declaration of conformity shall have the model structure set out in Annex IV and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VI. Such a declaration shall be continuously updated. It shall be made available in the language or languages required by the Member State in which the product with digital elements is placed on the market or made available **on the market**.

   The simplified EU declaration of conformity referred to in Article 10(11) shall contain the model structure set out in Annex [XX] and shall be continuously updated. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market. The full text of the EU declaration of conformity shall be available at the internet address referred to in the simplified EU declaration of conformity, in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market.

3. Where a product with digital elements is subject to more than one Union act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union acts. That declaration shall contain the identification of the Union acts concerned, including their publication references.

4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product.

[3] Will be updated according to Art 17 in the Machinery Regulation once it is finalised.

5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by adding elements to the minimum content of the EU declaration of conformity set out in Annex IV to take account of technological developments.

Article 21

General principles of the CE marking

The CE marking as defined in Article 3(32) shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

Article 22

Rules and conditions for affixing the CE marking

1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to ~~**the packaging and**~~**the accompanying documents and where applicable to the packaging** ~~**EU declaration of conformity referred to in Article 20 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product**~~.

2. On account of the nature of the product with digital elements, the height of the CE marking affixed to the product with digital elements may be lower than 5 mm, provided that it remains visible and legible.

3. The CE marking shall be affixed before the product with digital elements is placed on the market. It may be followed by a pictogram or any other mark indicating a special risk or use set out in implementing acts referred to in paragraph 6.

4. The CE marking shall be followed by the identification number of the notified body, where that body is involved in the conformity assessment procedure based on full quality assurance (based on module H) referred to in Article 24.

   The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised representative.

5. Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking. Where the product with digital elements is subject to other Union legislation which also provides for the affixing of the CE marking, the CE marking shall indicate that the product also fulfils the requirements of that other legislation.

6. The Commission may, by means of implementing acts, lay down technical specifications for pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Article 23

Technical documentation

1. The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential requirements set out in Annex I. It shall at least contain the elements set out in Annex V.

2. The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated**~~, where appropriate, during the expected product lifetime or during a period of five years after the placing on the market of a product with digital elements, whichever is shorter~~**.

3. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, one single technical documentation shall be drawn up containing the information referred to in Annex V of this Regulation and the information required by those respective Union acts.

4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body.

5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by the elements to be included in the technical documentation set out in Annex V to take account of technological developments, as well as developments encountered in the implementation process of this Regulation.

Article 24

Conformity assessment procedures for products with digital elements

1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer **~~or the manufacturer's authorised representative~~** shall demonstrate conformity with the essential requirements by using **~~one~~ any** of the following procedures:

   (a) the internal control procedure (based on module A) set out in Annex VI; **~~or~~**

   (b) the EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; **~~or~~**

   (c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI**~~.~~ ; or**

   (d) where applicable, a European cybersecurity certification scheme as specified in Article 18(3) and (4) at any assurance level.

2. Where, in assessing the compliance of the critical product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer **~~or the manufacturer's authorised representative~~** has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to **~~either~~ any** of the following procedures:

   (a) **the** EU-type examination procedure (based on module B) **~~provided for~~ set out** in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; **~~or~~**

   (b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI**~~.~~; or**

   (c) where applicable, a European cybersecurity certification scheme as specified in Article 18(3) and (4) at assurance level 'substantial' or 'high'.

3. Where the product is a critical product with digital elements of class II as set out in Annex III, the manufacturer **~~or the manufacturer's authorised representative~~** shall demonstrate conformity with the essential requirements set out in Annex I by using **~~one~~ any** of the following procedures:

   (a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; **~~or~~**

   (b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI**~~.~~; or**

   (c) where applicable, a European cybersecurity certification scheme as specified in Article 18 (3) and (4) at assurance level 'substantial' or 'high'.

4. Manufacturers of products with digital elements that are classified as EHR systems under the scope of Regulation [the European Health Data Space Regulation] shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by Regulation [Chapter III of the European Health Data Space Regulation].

5. **~~Notified bodies shall take into account the specific interests and needs of small and medium sized enterprises (SMEs) when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs.~~ The specific interests and needs of SMEs[4], including start-ups, shall be taken into account when setting the fees for conformity assessment, reducing those fees proportionately to their size, market size and other relevant indicators.**

[4] A definition will be added.

[ANNEX III

CLASSES AND CATEGORIES OF CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class I

Categories of products with digital elements which meet the criteria referred to in Article 6(1), second subparagraph, point (a):

~~**1. Identity management systems software and privileged access management software;**~~

~~**2. Standalone and embedded browsers;**~~

~~**3. Password managers;**~~

1. ~~**4.**~~Software that searches for, removes, or quarantines malicious software;

~~**5. Products with digital elements with the function of virtual private network (VPN);**~~

~~**6. Network management systems;**~~

~~**7. Network configuration management tools;**~~

2. ~~**8.**~~Network traffic monitoring systems **for throughput and flow control**;

~~**9. Management of network resources;**~~

3. ~~**10**~~. Security information and event management (SIEM) systems;

4. ~~**11.**~~ **Update**/patch management, including boot managers;

5. ~~**17.**~~ Firewalls, intrusion detection and/or prevention systems not covered by class II;

6. ~~**3.**~~ **Public key infrastructure and digital certificate issu**~~**ers**~~**ance software;**

7. Smart home products with safety functionalities, such as door locks and alarm systems.

~~**12. Application configuration management systems;**~~

~~**13. Remote access/sharing software;**~~

~~**14. Mobile device management software;**~~

~~**15. Physical network interfaces;**~~

Categories of products with digital elements which meet the criteria referred to in Article 6(1), second subparagraph, point (b):

8. ~~16.~~Operating systems not covered by class II;

~~**17. Firewalls, intrusion detection and/or prevention systems not covered by class II;**~~

9. ~~2.~~ Standalone and embedded browsers;

10. ~~9.~~Management of network resources**, including software-defined networking (SDN) technology;**

11. ~~12.~~Application configuration management systems **for centralised systems configuration;**

12. ~~13.~~ Remote access/sharing software;

13. ~~14.~~ Mobile device management software **for the configuration, monitoring and updating of mobile devices;**

14. ~~15.~~ Physical **and virtual** network interfaces;

15. ~~18.~~ Routers, modems intended for the connection to the internet, and switches, not covered by class II;

16. ~~19.~~ Microprocessors ~~**not covered by class II,**~~ including general purpose microprocessors;

17. ~~20.~~ Microcontrollers;

~~**21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];**~~

18. ~~22.~~ Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);

19. ~~23.~~Industrial Internet of Things not covered by class II**;**

20. ~~14.~~ ~~Robot sensing and actuator components and~~ Industrial robot controllers.

Class II

Categories of products with digital elements which meet both the criteria referred to in Article 6(1), third subparagraph, points (a) and (b):

~~**1. Operating systems for servers, desktops, and mobile devices**~~;

1. Identity management systems software and privileged access management software;

2. Authentication tools; ~~Password managers~~

3. Products with digital elements with the function of virtual private network (VPN);

4. ~~6.~~ Network management systems for the configuration, monitoring and updating of network devices;

~~5. 2.~~ Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;

~~**3.Public key infrastructure and digital certificate issuers;**~~

~~**4.Firewalls, intrusion detection and/or prevention systems intended for industrial use;**~~

~~**5.General purpose microprocessors;**~~

6. Microprocessors intended for integration in programmable logic controllers and secure elements;

~~**7.Routers, modems intended for the connection to the internet, and switches, intended for industrial use;**~~

6. 8~~.~~ Devices based on tamper-resistant integrated circuits, including embedded and integrated Ssecure Eelements;

7. ~~9.~~ Hardware Security Modules (HSMs);

8. ~~10.~~ Secure cryptoprocessors;

9. ~~11.~~ Smartcards, smartcard readers and tokens.

Categories of products with digital elements which meet both the criteria referred to in Article 6(1), third subparagraph, points (a) and (c):

10. ~~4.~~ Firewalls, intrusion detection and/or prevention systems intended for industrial use**.**

Categories of products with digital elements which meet both the criteria referred to in Article 6(1), third subparagraph, points (b) and (c):

~~**8. Secure elements;**~~

~~**9. Hardware Security Modules (HSMs);**~~

~~**10. Secure cryptoprocessors;**~~

~~**11. Smartcards, smartcard readers and tokens;**~~

11. ~~**21.**~~ **Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];**

12. Industrial Automation & Control Systems (IACS) **and components** intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);

13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];

~~**14. Robot sensing and actuator components and robot controllers;**~~

14. ~~**15.**~~ Smart meters **as defined in Article 2(23) of Directive (EU) 2019/944**.**]**

ANNEX [XX]

Simplified EU declaration of conformity

The simplified EU declaration of conformity referred to in Article [10(11)] shall be provided as follows:

Hereby, [Name of manufacturer] declares that the product with digital elements type [designation of type of product with digital element] is in compliance with Regulation XX.

The full text of the EU declaration of conformity is available at the following internet address: