EUROPEAN
COMMISSION

Brussels, 3.2.2025
C(2025) 618 final

ANNEXES 1 to 2

**ANNEXES**

**to the**

**Commission Implementing Decision**

**on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)**

**ANNEX I**

**List of new European Standards to be drafted**

| Reference information | | Deadline for the adoption by the ESOs |
|---|---|---|
| Horizontal standards for security requirements relating to the properties of products with digital elements | | |
| 1. | European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks | 30/08/2026 |
| 2. | European standard(s) on making products with digital elements available on the market without known exploitable vulnerabilities | 30/10/2027 |
| 3. | European standard(s) on making products with digital elements available on the market with a secure by default configuration | 30/10/2027 |
| 4. | European standard(s) on ensuring that vulnerabilities in products with digital elements can be addressed through security updates | 30/10/2027 |
| 5. | European standard(s) on ensuring protection of products with digital elements from unauthorised access and reporting on possible unauthorised access | 30/10/2027 |
| 6. | European standard(s) on protecting the confidentiality of data stored, transmitted or otherwise processed by a product with digital elements | 30/10/2027 |
| 7. | European standard(s) on protecting the integrity of data, commands, programs by a product with digital elements, and its configuration against any manipulation or modification not authorised by the user, as well as reporting on corruptions | 30/10/2027 |
| 8. | European standard(s) on processing only personal or other data that are adequate, | 30/10/2027 |

| | | |
|---|---|---|
| | relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (‘minimisation of data’) | |
| 9. | European standard(s) on protecting the availability of essential and basic functions of the product with digital elements | 30/10/2027 |
| 10. | European standard(s) on minimising the negative impact of a product with digital elements or its connected devices on the availability of services provided by other devices or networks | 30/10/2027 |
| 11. | European standard(s) on designing, developing and producing products with digital elements with limitted attack surfaces | 30/10/2027 |
| 12. | European standard(s) on designing, developing and producing products with digital elements that reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques | 30/10/2027 |
| 13. | European standard(s) on providing security related information by recording and/or monitoring relevant internal activity of products with digital elements with an opt-out mechanism for the user | 30/10/2027 |
| 14. | European standard(s) on securely and easily removing or transferring all data and settings of a product with digital elements. | 30/10/2027 |
| Horizontal standards for vulnerability handling requirements | | |
| 15. | European standard(s) on vulnerability handling for products with digital elements | 30/08/2026 |
| Vertical standards for security requirements relating to the properties of products with digital elements | | |
| 16. | European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers | 30/10/2026 |

| | | |
|---|---|---|
| 17. | European standard(s) on essential cybersecurity requirements for standalone and embedded browsers | 30/10/2026 |
| 18. | European standard(s) on essential cybersecurity requirements for password managers | 30/10/2026 |
| 19. | European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software | 30/10/2026 |
| 20. | European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN) | 30/10/2026 |
| 21. | European standard(s) on essential cybersecurity requirements for network management systems | 30/10/2026 |
| 22. | European standard(s) on essential cybersecurity requirements for Security information and event management (SIEM) systems | 30/10/2026 |
| 23. | European standard(s) on essential cybersecurity requirements for boot managers | 30/10/2026 |
| 24. | European standard(s) on essential cybersecurity requirements for public key infrastructure and digital certificate issuance software | 30/10/2026 |
| 25. | European standard(s) on essential cybersecurity requirements for physical and virtual network interfaces | 30/10/2026 |
| 26. | European standard(s) on essential cybersecurity requirements for operating systems | 30/10/2026 |
| 27. | European standard(s) on essential cybersecurity requirements for routers, modems intended for the connection to the internet, and switches | 30/10/2026 |
| 28. | European standard(s) on essential cybersecurity requirements for | 30/10/2026 |

| | | |
|---|---|---|
| | microprocessors with security-related functionalities | |
| 29. | European standard(s) on essential cybersecurity requirements for microcontrollers with security-related functionalities | 30/10/2026 |
| 30. | European standard(s) on essential cybersecurity requirements for application specific integrated circuits (AS IC) and field-programmable gate arrays (FPGA) with security-related functionalities | 30/10/2026 |
| 31. | European standard(s) on essential cybersecurity requirements for smart home general purpose virtual assistants | 30/10/2026 |
| 32. | European standard(s) on essential cybersecurity requirements for smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems | 30/10/2026 |
| 33. | European standard(s) on essential cybersecurity requirements for Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features | 30/10/2026 |
| 34. | European standard(s) on essential cybersecurity requirements for personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply or personal wearable products that are intended for the use by and for children | 30/10/2026 |
| 35. | European standard(s) on essential cybersecurity requirements for hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments | 30/10/2026 |
| 36. | European standard(s) on essential cybersecurity requirements for firewalls, | 30/10/2026 |

| | | |
|---|---|---|
| | intrusion<br>detection and/or prevention systems,<br>including specifically those intended for industrial use | |
| 37. | European standard(s) on essential cybersecurity requirements for tamper-resistant microprocessors | 30/10/2026 |
| 38. | European standard(s) on essential cybersecurity requirements for tamper-resistant microcontrollers | 30/10/2026 |
| 39. | European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes | 30/10/2026 |
| 40. | European standard(s) on essential cybersecurity requirements for smart meter gateways within smart metering systems as defined in Article 2 (23) of Directive (EU) 2019/944 and other devices for advanced security purposes, including for secure cryptoprocessing | 30/10/2026 |
| 41. | European standard(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements | 30/10/2026 |

## ANNEX II

## Requirements for the European standards referred to in Article 1

### 1. Requirements for the requested European standards

*Objectives*

The harmonised European standards shall reflect the generally acknowledged state of the art[1] in order to minimise the cybersecurity risks which arise in the planning, design, development, production, delivery and maintenance of products with digital elements, aiming to prevent security incidents and minimise the impacts of such incidents, including in relation to the health and safety of users.

The harmonised European standards shall provide, to the extent necessary and reflecting the state of the art, technology-, process- or methodology-based technical specifications in relation to the design and development of products with digital elements, including evaluation procedures such as testing and review, with objectively verifiable criteria and implementable methods to assess compliance with such specifications.

Supporting specifications or other standardisation deliverables (e.g. on terminology[2]) shall be identified and provided when necessary to ensure the consistency and implementation of the European standards. Such supporting specifications may also include elements useful for the horizontal and vertical standards, such as catalogues of security controls, threats, vulnerabilities, attack methods, specifications on communication and instructions to users, as well as provisions relating to accessibility.

*Coherence*

The harmonised standards developed in response to this request should build on the work currently under development to support Commission Delegated Regulation (EU) 2022/30[3], without prejudice to needed improvements. The specificities of Regulation (EU) 2024/2847[4] shall however be fully addressed during the development stage. Where possible, CEN, Cenelec and ETSI may update already existing standards and standardisation deliverables to align with the requirements of the Cyber Resilience Act.

Without prejudice to needed improvements, CEN, Cenelec and ETSI shall ensure that the European standards produced are consistent, when applicable, with other European and harmonised standards developed or under development in the various relevant sectors, notably

---

1 The state of the art does not necessarily imply the latest scientific research still in an experimental stage or with insufficient technological maturity. The state-of-the-art is not to be intended as minimum requirements to access the market.

2 All the European Standards elaborated on the basis of this request shall rely on a common set of terms. Moreover, supporting specifications on terminology shall build as much as possible on terminology adopted at international level and notably in international standards.

3 Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (OJ L 7, 12.1.2022, p. 6, ELI: http://data.europa.eu/eli/reg_del/2022/30/oj).

4 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj)

those related to products covered by EU legislation such as Directive 2006/42/EC of the European Parliament and of the Council[5], Regulation (EU) 2023/1230[6], (EU) 2024/1689[7] , (EU) 2023/1781[8], or EU cybersecurity certification schemes developed or under development under Regulation (EU) 2019/881 of the European Parliament and of the Council[9]. Furthermore, CEN, Cenelec and ETSI should ensure that harmonised standards produced in response to this Decision are consistent with Union obligations under international agreements and treaties.

*Scope of the European standards*

Each harmonised European standard shall clearly indicate its scope, the products which fall under its scope, which risks are covered, and which other relevant risks are not covered. Where a harmonised European standard does not cover all the essential requirements which are applicable to the products falling under its scope, it shall indicate the essential requirements not fully covered. Where a harmonised European Standard does not mitigate risks identified following a comprehensive analysis, which relate to one of the essential requirements it aims to cover and which apply to the products falling under its scope, that standard shall indicate the risks not mitigated and provide, to the extent possible, non-normative information on which other way such risks could be addressed.

The requested harmonised standards shall include at least provisions related to the security problem definition, security objectives, technical specification of security requirements, assessment methodology.

In terms of security problem definition, the requested harmonised standards shall be transparent as to the threats they cover, the policies and assumptions they are based on, and shall support manufacturers in carrying out identification and specification of threats, policies and assumptions. This may for instance be achieved through the development or referencing of existing catalogues of security controls, threats, attack methods, and vulnerabilities, and a discussion on reasonable assumptions.

The security objectives shall define the scope of the target product or service and the security properties it is intended to address, based on the essential requirements set out in the Cyber

---

5 Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24, ELI: http://data.europa.eu/eli/dir/2006/42/oj).

6 Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (OJ L 165, 29.6.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1230/oj).

7 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

8 Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (OJ L 229, 18.9.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1781/oj).

9 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

Resilience Act. The normative statements made in the harmonised standard shall concisely express the intended solution to the identified risks (security problem). The method used to identify the security objectives shall rely on existing standards defining risk analysis approaches. The harmonised standards are expected to include the relation between the security objectives and the identified risks (security problem).

The specification of security requirements describes the desired cybersecurity behaviour expected for the target product or service. Where feasible, the standards shall cover a variety of security levels catering to different expected market needs, such as different intended purposes, operational environments or categories of users (for example, consumer, enterprise, critical).

The assessment methodology shall consist of a set of evaluation procedures required to assess the target against the technical specification requirements identified previously. It defines "how" to evaluate the target to prove the required level of security. It shall cover at least the definition of the concept of evaluation methodology, definition of the concept of composition methodology (when relevant), and definition of the expected evaluation results.

All requested harmonised European standards developed under this Decision shall be drafted in such a way that they may facilitate publication in the *Official Journal of the European Union*.

## 2. Requirements for specific European Standards

### 2.1 Horizontal cybersecurity standards relating to the properties of products with digital elements (entries 1-14 in Annex I)

The development of horizontal harmonised standards addressing different aspects and mechanisms of product cybersecurity shall support (i) the development of further, granular vertical harmonised standards for specific products or product types, and (ii) shall support manufacturers in defining and implementing the security requirements applicable to their respective products, including particularly for products not covered by existing or planned vertical standards. Deviations from the horizontal harmonised standards shall be duly justified.

The harmonised European standard on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks (entry 1 in Annex I) shall serve as a framework covering all elements defined in section 1 of this Annex, and shall set out the main elements that shall be contained in other product security standards for the Cyber Resilience Act.

Rather than focus only on the minimum common aspects, the horizontal harmonised standards shall strive to provide a broad and useful overview of the relevant security mechanisms that can apply to products within the scope of the Cyber Resilience Act. Wherever relevant, the requested harmonised European standards shall include provisions on secure software development. The standard shall therefore ensure clarity on the scope of each normative statement.

When considering the scope of products to be covered under the Cyber Resilience Act for the purposes of the development of horizontal standards, CEN, Cenelec and ETSI shall where appropriate take into consideration that the essential requirements laid down in Annex I of the proposed Cyber Resilience Act will apply to products with digital elements that are also in the scope of other Union legislation, such as electronic health record systems, high-risk AI systems under Regulation (EU) 2024/1689, machinery products under Directive 2006/42/EC

of the European Parliament and of the Council and Regulation (EU) 2023/1230, or trusted chips under Regulation (EU) 2023/1781.

2.2 Vulnerability handling requirements for products with digital elements (entry 15 in Annex I)

The harmonised European standard(s) for vulnerability handling requirements shall provide specifications for vulnerability handling processes, covering all relevant product categories, to be put in place by manufacturers of the products with digital elements. Those processes shall allow the manufacturer to:

(a) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(b) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(c) apply effective and regular tests and reviews of the security of the product with digital elements;

(d) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(e) put in place and enforce a policy on coordinated vulnerability disclosure;

(f) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(g) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner, and, where applicable for security updates, in an automatic manner;

(h) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

2.3 Vertical cybersecurity standards relating to the properties of products with digital elements (entries 16 to 41 in Annex I)

The vertical harmonised European standards relating to the properties of products with digital elements shall provide specifications for the cybersecurity requirements of important or critical products as defined in Annex III and IV of the Cyber Resilience Act.

Vertical harmonised standards shall be used to implement and further develop the provisions of the requested horizontal standards listed in entries 1 to 15 of Annex I, while taking also into consideration relevant differences arising from intended purpose and reasonably foreseeable use. Given the timeline for the different deliverables, vertical standards shall ensure coherence with the horizontal standard on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks (entry 1 listen in Annex I) and where appropriate with the horizontal standard on vulnerability handling for products with digital elements (entry 15 listed in Annex I). The objective of alignment of the vertical standards with the horizontal standards listed in entries 2 to 14 of Annex I shall also be considered, with the expectation that standards shall converge through the regular process of review over time.

For those products covered in Annex IV of the Cyber Resilience Act for which technical domains or protection profiles exist, the developed harmonised standards shall take into account existing European cybersecurity certification schemes developed or under development under Regulation (EU) 2019/881, in particular the European Common Criteria-based cybersecurity certification scheme (EUCC).

The vertical harmonised standards developed for this request (entries 16 to 41 in Annex I) focusing specifically on products subject to third party conformity assessment (important or critical products) shall set forth a risk-based approach to assurance such that lower risk use cases may be subject to validation procedures only, but higher risk use cases would be subject to (increasingly) higher forms of verification procedures.

Those harmonised European standards shall adequately cover the relevant risks identified for a given intended purpose or reasonably foreseeable use, and shall therefore be based on a comprehensive risk analysis carried out in the development of each harmonised standard.

In addition, the development of vertical harmonised standards covering a broad scope of products or product categories (such as operational technology), may support and facilitate the structured and coherent development of product-specific vertical harmonised standards as referred in this Request, as long as there is no ambiguity on the requirements, the scope, the covered risks and the non-covered risks. Such broad vertical harmonised standards shall provide at least partial coverage of the risks associated to a specific intended purpose and reasonably foreseeable use, and shall be complemented by further, more granular and product-specific, vertical harmonised standards aiming to provide presumption of conformity for a more reduced product scope, covering the additional or specific risks associated to that scope and its relevant intended purposes and reasonably foreseeable uses.