EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

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

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021. Such products suffer from two major problems adding costs for users and the society: (1) a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and (2) an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner. In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. This can lead to severe disruption of economic and social activities or even become life threatening.

The cybersecurity of products with digital elements has a strong cross-border dimension, as products manufactured in one country are often used across the internal market. In addition, incidents initially affecting a single entity or a single Member State often spread within minutes across the entire internal market.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs. There are numerous examples of noteworthy cyberattacks resulting from suboptimal product security, such as the WannaCry ransomware worm, which exploited a Windows vulnerability that affected 200 000 computers across 150 countries in 2017 and caused a damage amounting to billions of USD; the Kaseya VSA supply chain attack, which used Kaseya's network administration software to attack over 1 000 companies and forcing a supermarket chain to close all its 500 shops across Sweden; or the many incidents in which banking applications are hacked to steal money from unsuspecting consumers.
Two main objectives were identified aiming to ensure the proper functioning of the internal market: (1) create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and (2) create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. Four specific objectives were set out: (i) ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle; (ii) ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers; (iii) enhance the transparency of security properties of products with digital elements, and (iv) enable businesses and consumers to use products with digital elements securely.

The strong cross-border nature of cybersecurity and the growing incidents, with spill-over effects across borders, sectors and products, mean that the objectives cannot effectively be achieved by Member States alone. Given the global nature of markets for products with digital elements, Member States face the same risks for the same product with digital

elements on their territory. An emerging fragmented framework of potentially diverging national rules risks hampering an open and competitive single market for products with digital elements. Joint action at EU level is thus necessary to increase the level of trust among users and the attractiveness of EU products with digital elements. It would also benefit the internal market by providing legal certainty and achieving a level playing field for vendors of products with digital elements, as highlighted also in the final report of the Conference on the Future of Europe, in which citizens call for a stronger role for the EU in countering cybersecurity threats.

- **Interplay with existing policy provisions in the policy area**

The EU framework comprises several pieces of horizontal legislation that cover certain aspects linked to cybersecurity from different angles (products, services, crisis management, and crimes). In 2013, the Directive on attacks against information systems,[1] harmonising criminalisation and penalties for a number of offences directed against information systems came into force. In August 2016, Directive (EU) 2016/1148 on security of network and information systems (NIS Directive)[2] entered into force as the first piece of EU-wide legislation on cybersecurity. Its revision, resulting in Directive [Directive XXX/XXXX (NIS2)], raises the EU common level of ambition. In 2019, the EU Cybersecurity Act[3] entered into force, aiming to enhance the security of ICT products, ICT services and ICT processes by introducing a voluntary European cybersecurity certification framework.[4]
Cybersecurity of the entire supply chain is ensured only if all its components are cyber-secure. The above-mentioned EU legislation has however substantial gaps in this regard, as it does not cover mandatory requirements for the security of products with digital elements.
While the proposed Cyber Resilience Act covers products with digital elements placed on the market, the Directive [Directive XXX/XXX (NIS2)] aims at ensuring a high level of cybersecurity of services provided by essential and important entities. Directive [Directive XXX/XXXX (NIS2)] requires Member States to ensure that essential and important entities within the scope, such as health care or cloud providers and public administration entities, take appropriate and proportionate technical, operational and organisational cybersecurity measures. This includes, among others, a requirement to ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure. Directive [Directive XXX/XXXX (NIS2)] requires the Commission to adopt implementing acts laying down the technical and the methodological requirements of those measures within 21 months after the date of entry into force of this Directive for certain types of entities, such as cloud computing service providers. For all other entities, the Commission may adopt an implementing act, laying down the technical and the methodological requirements, as well as sectoral requirements. This framework will ensure that technical specifications and measures similar to the essential cybersecurity requirements

[1] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA OJ L 218, 14.8.2013, p. 8–14.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1).

[3] 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).

[4] The Cybersecurity Act allows the development of dedicated certification schemes. Each scheme includes references to relevant standards, technical specifications or other cybersecurity requirements defined in the scheme. The decision to develop a cybersecurity certification is a risk-based one.

of the Cyber Resilience Act are also implemented for the design, development and vulnerability handling of software provided as a service (Software-as-a-Service). For example, this could be a means to ensure a high level of cybersecurity in cases such as electronic health records (EHR) systems, including when delivered as Software-as-a-Service (SaaS) or developed within health institutions (in-house), in accordance with the proposed [European Health Data Space Regulation].

- **Interplay with other Union policies**

As set out in the Communication 'Shaping Europe's digital future'[5], it is crucial for the EU to reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe and ethical boundaries. The European strategy for data sets out four pillars – data protection, fundamental rights, safety and cybersecurity – as essential pre-requisites for a society empowered by the use of data.

The current EU framework[6] applicable to products that may also have digital elements comprises several pieces of legislation, including EU legislation on specific products covering safety-related aspects and general legislation on product liability. The proposal is coherent with the current product-related EU regulatory framework, as well as with recent legislative proposals such as the Commission's proposal for Regulation [the Artificial Intelligence (AI) Regulation][7].

The proposed Regulation would apply to all radio equipment within the scope of Commission Delegated Regulation (EU) 2022/30. Moreover, the requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU, including the main elements set out in the [Commission implementation decision XXX/2022 on a standardisation request to the European Standardisation Organisations] issued on the basis of that Delegated Regulation. In order to avoid a regulatory overlap, it is envisaged that the Commission would repeal or amend the Delegated Regulation with respect to the radio equipment covered by the proposed Regulation, so that the latter one would apply to it, once applicable.

Moreover, in order to avoid a duplication of work, it is envisaged that the Commission and the European Standardisation Organisations take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of the Regulation.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The legal basis for this proposal is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides for the adoption of measures to ensure the establishing and functioning of the internal market. The purpose of the proposal is to

---

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Shaping Europe's digital future" of 19 February 2020, COM(2020) 67 final.

6 Mainly New Legislative Framework (NLF) legislation.

7 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts of 21 April 2021, COM (2021) 206 final.

harmonise cybersecurity requirements for products with digital elements in all Member States and to remove obstacles to the free movement of goods.

Article 114 TFEU may be used as a legal basis to prevent the occurrence of these obstacles resulting from diverging national laws and approaches on how to address the legal uncertainties and gaps in the existing legal frameworks.[8] Furthermore, the Court of Justice has recognised that applying heterogeneous technical requirements could be valid grounds to trigger Article 114 TFEU.[9]

The current EU legislative framework applicable to products with digital elements is based on Article 114 TFEU, and comprises several pieces of legislation, including on specific products and safety-related aspects or general legislation on product liability. However, it covers only certain aspects linked to the cybersecurity of tangible digital products and, as applicable, software embedded in these products. At national level, Member States are starting to take national measures requiring vendors of digital products to enhance their cybersecurity.[10] At the same time, the cybersecurity of digital products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. Incidents that initially concern a single entity or Member State often spread within minutes across organisations, sectors and several Member States.

The various acts and initiatives taken so far at EU and national levels only partially address the problems identified and risk creating a legislative patchwork within the internal market, increasing legal uncertainty for both vendors and users of these products and adding unnecessary burden on companies to comply with a number of requirements for similar types of products.

The proposed Regulation would harmonise and streamline the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements and avoid overlapping requirements stemming from different pieces of legislation. This would create greater legal certainty for operators and users across the Union, as well as a better harmonisation of the European single market, creating more viable conditions for operators aiming at entering the EU market.

- **Subsidiarity (for non-exclusive competence)**

The strong cross-border nature of cybersecurity in general and the growing number of risks and incidents, which have spill-over effects across borders, sectors and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone. National approaches in addressing the problems, and in particular approaches introducing mandatory requirements, will create additional legal uncertainty and legal barriers. Companies could be prevented from seamlessly expanding into other Member States, depriving users of the benefits of their products.

Joint action at EU level is therefore necessary to establish a high level of trust among users, increasing the attractiveness of EU products with digital elements. It would also benefit the

8 CJEU Judgment of the Court (Grand Chamber) of 3 December 2019, Czech Republic v European Parliament and Council of the European Union, Case C-482/17, paragraph 35.

9 CJEU Judgment of the Court (Grand Chamber) of 2 May 2006, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union, Case C-217/04, paragraphs 62-63.

10 For example, in 2019, Finland has created a labelling scheme for IoT devices, such as smart TVs, smartphones and toys based on the ETSI standards. Germany has recently introduced a consumer security label for broadband routers, smart TVs, cameras, speakers, toys, as well as cleaning and gardening robots.

digital single market and internal market in general by providing legal certainty and achieving a level playing field for manufacturers of products with digital elements.
Ultimately, the Council Conclusions of 23 May 2022 on the development of the European Union's cyber posture call upon the Commission to propose, by the end of 2022, common cybersecurity requirements for connected devices.

- **Proportionality**

As regards the proportionality of the proposed Regulation, the measures in the policy options considered would not go beyond what is needed to achieve the general and specific objectives and would not impose disproportionate costs. More specifically, the intervention considered would ensure that products with digital elements would be secured throughout their whole life cycle and proportionally to the risks faced through objective-oriented and technology neutral requirements that remain reasonable and generally corresponding to the interest of the entities involved.
The essential cybersecurity requirements in the proposal are building on widely used standards, and the standardisation process that will follow would take into account the technical specificities of the products. This means that where needed for a given risk level, security controls would be adapted. Furthermore, the envisaged horizontal rules would only foresee third-party assessment for critical products. This would only include a narrow share of the market for products with digital elements. The impact on SMEs would depend on their presence in the market of these specific product categories.
Regarding the proportionality of the costs for conformity assessment, notified bodies conducting the third party assessments would take the size of the undertaking into account when setting their fees. A reasonable transition period of 24 months to prepare the implementation would also be provided , giving time to the relevant markets to prepare, while providing a clear direction for R&D investments. Any compliance costs for businesses would be outweighed by the benefits brought by a higher level of security of products with digital elements and ultimately an increase of trust of users in these products.

- **Choice of the instrument**

A regulatory intervention would entail the adoption of a regulation and not a directive. This is because, for this particular type of product legislation, a regulation would more effectively address the problems identified and meet the objectives formulated, since it is an intervention that is conditioning the placing on the internal market of a very wide category of products. The transposition process in the case of a directive for such intervention could leave too much room for discretion at national level, potentially leading to lack of uniformity of certain essential cybersecurity requirements, legal uncertainty, further fragmentation or even discriminatory situations cross-border, even more taking account of the fact that the products covered could be of multiple purpose or use and that manufacturers can produce multiple categories of such products.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

The Commission has consulted a broad range of stakeholders. Member States and stakeholders were invited to participate in the open public consultation and in the surveys and workshops organised in the context of a study conducted by a consortium supporting the Commission's preparatory work for the impact assessment: Wavestone, the Centre for European Policy Studies (CEPS) and ICF. The consulted stakeholders included national

market surveillance authorities, Union bodies dealing with cybersecurity, hardware and software manufacturers, importers and distributors of hardware and software, trade associations, consumer organisations and users of products with digital elements and citizens, researchers and academia, notified bodies and accreditation bodies, and cybersecurity industry professionals.

Consultation activities included:

- A first study conducted by a consortium consisting of ICF, Wavestone, Carsa and CEPS, which was published in December 2021[11]. The study identified several market failures and assessed possible regulatory interventions.
- An Open Public Consultation that targeted citizens, stakeholders and cybersecurity experts. 176 replies were submitted. These contributed to the collection of diverse opinions and experiences from all stakeholder groups.
- Workshops organised by the study supporting the Commission's preparatory work for a Cyber Resilience Act gathered around 100 representatives from all 27 Member States representing a variety of stakeholders.
- Expert interviews were conducted to gain a deeper understanding of current cybersecurity challenges related to products with digital elements, and to discuss policy options for a potential regulatory intervention.
- Bilateral discussions were held with national cybersecurity authorities, the private sector, and consumer organisations.
- Targeted outreach was done to key SME stakeholders.

- **Collection and use of expertise**

The consultation activities aimed to obtain input on the five main evaluation criteria based on the EU Better Regulation Guidelines (effectiveness, efficiency, relevance, coherence, EU-added value) as well as the potential impacts of possible options for the future. The contractor has not only reached out to the stakeholders that would be directly affected by the proposed Regulation, but has also consulted with a wide range of experts in the field of cybersecurity.

- **Impact assessment**

The Commission conducted an impact assessment for this proposal examined by the Commission's Regulatory Scrutiny Board (RSB). A meeting with the RSB was held on July 6th 2022 and was followed by a positive opinion. The Impact Assessment was adjusted to address the recommendations and comments of the RSB.

The Commission examined different policy options to achieve the general objective of the proposal:

- Soft law approach and voluntary measures (option 1): In this option, there would be no mandatory regulatory intervention. Instead, the Commission would issue communications, guidance, recommendations and potentially codes of conduct to encourage voluntary measures. National schemes,

[11] Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715, Final Study Report, available under https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

voluntary or mandatory, would continue to be developed to compensate for the lack of EU horizontal rules.

- Ad-hoc regulatory intervention for cybersecurity of tangible products with digital elements and respective embedded software (option 2): This option would entail an ad-hoc product-specific regulatory intervention that would be limited to adding and/or amending the cybersecurity requirements in the already existing legislation or introducing new legislation as new risks emerge, including potentially on non-embedded software.

The options 3 and 4 entail a horizontal regulatory intervention varying in scope, largely following the New Legislative Framework (NLF). This framework sets out essential requirements as a condition for the placement of certain products on the internal market. The NLF also typically provides for conformity assessment, the process conducted by the manufacturer to demonstrate whether specified requirements relating to a product have been fulfilled.

- Mixed approach, including horizontal mandatory rules for cybersecurity of tangible products with digital elements and respective embedded software and a staggered approach for non-embedded software (option 3): This option would entail a regulation introducing horizontal cybersecurity requirements for all tangible products with digital elements and the software embedded within these, as a condition for placement on the market, and would include two sub-options with and without mandatory third-party assessment (3i and 3ii). Non-embedded software would not be regulated.

- A horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of tangible and non-tangible products with digital elements, including non-embedded software (option 4): This option resembles option 3, apart from the scope. Option 4 would include non-embedded software (with two sub-options respectively including only critical (4a) or all software (4b)) in the scope of a potential regulation. For each sub-option, the same sub-options related to conformity assessment as for option 3 would be considered.

Option 4 (with sub-options covering all software and involving mandatory third-party assessment for critical products) emerged as the preferred option based on the assessment of effectiveness against the specific objectives and efficiency of costs versus benefits. This option would ensure the setting out of specific horizontal cybersecurity requirements for all products with digital elements being placed or made available on the internal market, and would be the only option covering the entire digital supply chain. Non-embedded software, often exposed to vulnerabilities, would also be covered by such regulatory intervention, thus ensuring a coherent approach towards all products with digital elements, with a clear share of responsibilities of various economic operators.
This policy option also brings added value by covering duty of care and whole life cycle aspects after the placement of the products with digital elements on the market, to ensure, among others, appropriate information on security support and provision of security updates. This policy option would also come to most effectively complement the recent review of the NIS framework, by ensuring the prerequisites for a strengthened supply chain security.
The preferred option would bring significant benefits to the various stakeholders. For businesses, it would prevent divergent security rules for products with digital elements and decrease compliance costs for related cybersecurity legislation. It would reduce the number of cyber incidents, incident handling costs and reputational damage. For the whole EU, it is estimated that the initiative could lead to a costs reduction from incidents affecting companies

by roughly EUR 180 to 290 billion annually. It would lead to an increased turnover due to uptake of products with digital elements demand. It would improve the companies' global reputation leading to a demand uptake also outside the EU. For users, the preferred option would enhance the transparency of the security properties and facilitate the use of products with digital elements. Consumers and citizens would also benefit from better protection of their fundamental rights, such as privacy and data protection.
When asked to rate the effectiveness of the policy interventions, the public consultation respondents agreed that option 4 would be the most effective measure (4.08 on a scale from 1 to 5). This includes consumer organisations (5.00), respondents identifying themselves as users (4.22), notified bodies (4.17), market surveillance authorities (5.00) and producers of products with digital elements (3.85), including those of small and medium size (4.05).

- **Regulatory fitness and simplification**

This proposal lays down requirements that will apply to manufactures of software and hardware. There is a need to ensure legal certainty and avoid further market fragmentation of product-related requirements on cybersecurity on the internal market, which has been demonstrated by the broad support of various stakeholders for a horizontal intervention. The proposal will minimise the regulatory burden put on manufacturers by several product safety acts. The alignment to the NLF means a better functioning of the intervention and its enforcement. The proposal streamlines the process of safeguard procedures, by involving manufacturers and Member States before the Commission is notified. A large part of manufacturers in the scope of the proposal is already familiar with the workings of the NLF, which will contribute to its understanding and implementation. For consumers and companies the Proposal will promote trust in products with digital elements.

- **Fundamental rights**

All policy options are expected to enhance to a certain extent the protection of fundamental rights and freedoms such as privacy, protection of personal data, freedom to conduct business and protection of property or personal dignity and integrity. In particular the preferred policy option 4 consisting of horizontal regulatory interventions and a broad policy scope, would be the most effective in this regard, as it is more likely to help decrease the number and severity of incidents, including personal data breaches. It would also increase the legal certainty and achieve a level playing field for economic operators, raise trust among users and the attractiveness of EU products with digital elements as a whole, thus protecting the property and improving the conditions for economic operators to conduct business.
The horizontal cybersecurity requirements would contribute to the security of personal data by protecting the confidentiality, integrity and availability of information in products with digital elements. Compliance with those requirements will facilitate compliance with the requirement of security of processing of personal data under Regulation (EU) 2016/679 on the General Data Protection Regulation (GDPR)[12]. The proposal would enhance the transparency and information to users, including those that might be less equipped with cybersecurity skills. Users would also be better informed about the risks, capabilities and limitations of the products with digital elements, which would place them in a better position to take the necessary preventive and mitigating measures to reduce the residual risks.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

4. BUDGETARY IMPLICATIONS

In order to meet the tasks allocated to the European Union Agency for Cybersecurity (ENISA) under this Regulation, ENISA will have to re-allocate resources of approximately 4.5 FTEs. The Commission would need to allocate 7 FTEs to meet its responsibilities related to enforcement under this Regulation.
A detailed overview of the costs involved is provided in the 'financial statement' linked to this proposal.

5. OTHER ELEMENTS

• Implementation plans and monitoring, evaluation and reporting arrangements

The Commission will monitor the implementation, the application and the compliance to these new provisions with a view to assessing their effectiveness. The regulation will request a Commission's evaluation and review and the submission of a public report in this respect to the European Parliament and to the Council by 36 months after the date of application and every four years thereafter.

• Detailed explanation of the specific provisions of the proposal

General provisions (Chapter I)

This proposed Regulation lays down (a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products; (b) 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; (c) 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; (d) rules on market surveillance and enforcement of the above-mentioned rules and requirements.
The proposed Regulation will apply to all products with digital elements whose intended and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.
The proposed Regulation will not apply to products with digital elements within the scope of Regulation (EU) 2017/745 [medical devices for human use and accessories for such devices] and Regulation (EU) 2017/746 [in vitro diagnostic medical devices for human use and accessories for such devices], as both Regulations contain requirements regarding devices, including on software and general obligations on manufacturers, covering the whole life cycle of products, as well as conformity assessment procedures. This Regulation will not apply to products with digital elements that have been certified in accordance with Regulation 2018/1139 [high uniform level of civil aviation safety], nor to products to which Regulation (EU) 2019/2144 applies [on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles].
Critical products with digital elements shall be subject to specific conformity assessment procedures and shall be divided into class I and class II as set out in Annex III, reflecting their cybersecurity risk level, with class II representing a greater risk. A product with digital elements is considered critical and therefore included in Annex III taking into account the impact of potential cybersecurity vulnerabilities included in the product with digital elements. The cybersecurity-related functionality of the product with digital elements and the intended use in sensitive environments such as an industrial setting, amongst others, is taken into account in the determination of cybersecurity risk.

The Commission is also empowered to adopt delegated acts 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 under a European cybersecurity certification scheme 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 level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria considered for the listing of critical products with digital elements in Annex III as well as in view of the assessment of whether that category of products is used or relied upon by the essential entities of the type referred to in Annex [Annex I] to the Directive [Directive XXX/ XXXX (NIS2)] or will have potential future significance for the activities of these entities; or relevant for the resilience of the overall supply chain of products with digital elements against disruptive events.

Obligations of economic operators (Chapter II)

The proposal incorporates obligations for manufacturers, importers and distributors based on the reference provisions foreseen in Decision 768/2008/EC. The essential cybersecurity requirements and obligations mandate that all products with digital elements shall only be made available on the market if, where dully supplied, properly installed, maintained and used for their intended purpose or under conditions, which can be reasonably foreseen, they meet the essential cybersecurity requirements set out in this Regulation.

The essential requirements and obligations would mandate manufacturers to factor in cybersecurity in the design and development and production of the products with digital elements, exercise due diligence on security aspects when designing and developing their products, be transparent on cybersecurity aspects that need to be made known to customers, ensure security support (updates) in a proportionate way, and comply with vulnerability handling requirements.

Obligations would be set up for economic operators, starting from manufacturers, up to distributors and importers, in relation to the placement on the market of products with digital elements, as adequate for their role and responsibilities on the supply chain.

Conformity of the product with digital elements (Chapter III)

The product with digital elements, which is 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 of this proposed Regulation. Where harmonised standards do not exist or are insufficient or where there undue delays in the standardisation procedure or where the request by the Commission has not been accepted by the European standardisation organisations, the Commission may, by the means of implementing acts, adopt common specifications.

In addition, products with digital elements that have been certified or for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881, and for which the Commission specified via implementing act that it can provide presumption of conformity for this Regulation, shall be presumed to be in conformity with the essential requirements of this Regulation, or parts thereof, in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.

Furthermore, in order to avoid undue administrative burden for manufacturers, where applicable, the Commission should specify if a cybersecurity certificate issued under such a European cybersecurity certification scheme eliminates the obligation for manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements.

The manufacturer shall perform a conformity assessment of the product with digital elements and the vulnerability handling processes it has put in place to demonstrate conformity with the

essential requirements set out in Annex I by following one of the procedures set out in Annex VI. Manufactures of critical products of class I and II shall use the respective modules necessary for the compliance. Manufacturers of critical product of class II have to involve a third-party in their conformity assessment.

Notification of conformity assessment bodies (Chapter IV)

Proper functioning of notified bodies is crucial for ensuring a high level of cybersecurity and for the confidence of all interested parties in the New Approach system. Therefore, in line with the Decision 768/2008/EC, the proposal sets out requirements for national authorities responsible for conformity assessment bodies (notified bodies). It leaves the ultimate responsibility for designating and monitoring notified bodies with the Member States. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies.

Market surveillance and enforcement (Chapter V)

In accordance with Regulation (EU) 2019/1020, national market surveillance authorities carry out market surveillance in the territory of that Member State. Member States may choose to designate any existing or new authority to act as market surveillance authority, including national competent authorities established referred to in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] or designated national cybersecurity certification authorities referred to in Article 58 of Regulation (EU) 2019/881. Economic operators are asked to fully cooperate with market surveillance authorities and other competent authorities.

Delegated powers and committee procedures (Chapter VI)

In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU is delegated to the Commission for updating the list of critical products of class I and II and specifying the definitions of these products; specifying whether a limitation or exclusion is necessary for products with digital elements covered by other Union rules laying down requirements achieving the same level of protection as this Regulation; mandating the certification of certain highly critical products with digital elements based on criteria set out in this Regulation; specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation.

The Commission is also empowered to adopt implementing acts to: specify the format or elements of the reporting obligations and of the software bill of materials; specify the European cybersecurity certification schemes that can be used to demonstrate conformity with the essential requirements or parts thereof as set out in this Regulation; adopt common specifications; lay down technical specifications for the affixing of CE marking; adopt corrective or restrictive measures at Union level in exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market.

Confidentiality and penalties (Chapter VII)

All parties that apply this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities.

In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. In the same vein, this Regulation establishes maximum levels for administrative fines that should be provided in national laws for non-compliance with the obligations laid down in this Regulation.

Transitional and final provisions (Chapter VIII)

To allow manufacturers, notified bodies and Member States time to adapt to the new requirements, the proposed Regulation will become applicable [24 months] after its entry into force, except for the reporting obligation on manufacturers, which would apply from [12 months] after the date of entry into force.

2022/0272 (COD)

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

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee[1],
Having regard to the opinion of the Committee of the Regions[2],
Acting in accordance with the ordinary legislative procedure,
Whereas:

(1) It is necessary to improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

(2) This Regulation aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

(3) The relevant Union legislation that is currently in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, the existing Union legislation related to cybersecurity, including [Directive XXX/XXXX (NIS2)] and Regulation (EU) 2019/881 of the European Parliament and of the Council[3] does not directly cover mandatory requirements for the security of products with digital elements.

---

1 OJ C , , p. .
2 OJ C , , p. .
3 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

(4) While the existing Union legislation applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on companies to comply with a number of requirements for similar types of products. The cybersecurity of these products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level. The Union regulatory landscape should be harmonised by introducing cybersecurity requirements for products with digital elements. In addition, certainty for operators and users should be ensured across the Union, as well as a better harmonisation of the single market, creating more viable conditions for operators aiming at entering the Union market.

(5) At Union level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade[4], the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021,[5] have called for specific Union cybersecurity requirements for digital or connected products, with several countries around the world introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe,[6] citizens called for "a stronger role for the EU in countering cybersecurity threats".

(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally.

(7) Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered as less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or move laterally across systems. Manufacturers should therefore ensure that all connectable products with digital elements are designed and developed in accordance with essential requirements laid down in this Regulation. This includes both products that can be connected physically via hardware interfaces and products that are connected logically, such as via network sockets, pipes, files, application programming interfaces or any other types of software interface. As cybersecurity threats can propagate through various products with digital elements before reaching a certain target, for example by chaining together multiple vulnerability exploits, manufacturers should also ensure the cybersecurity of those products that are only indirectly connected to other devices or networks.

---

cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html.

6 *Conference on the Future of Europe – Report on the Final Outcome*, May 2022, Proposal 28(2). The Conference was held Between April 2021 and May 2022. It was a unique, citizen-led exercise of deliberative democracy at the pan-European level, involving thousands of European citizens as well as political actors, social partners, civil society representatives and key stakeholders.

(8) By setting cybersecurity requirements for placing on the market products with digital elements, the cybersecurity of these products for consumers and for businesses alike will be enhanced. This also includes requirements for placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitors.

(9) This Regulation ensures a high level of cybersecurity of products with digital elements. It does not regulate services, such as Software-as-a-Service (SaaS), except for remote data processing solutions relating to a product with digital elements understood as any data processing at a distance for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions. [Directive XXX/XXXX (NIS2)] puts in place cybersecurity and incident reporting requirements for essential and important entities, such as critical infrastructure, with a view to increasing the resilience of the services they provide. [Directive XXX/XXXX (NIS2)] applies to cloud computing services and cloud service models, such as SaaS. All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope of that Directive.

(10) In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

(11) A secure Internet is indispensable for the functioning of critical infrastructures and for society as a whole. [Directive XXX/XXXX (NIS2)] aims at ensuring a high level of cybersecurity of services provided by essential and important entities, including digital infrastructure providers that support core functions of the open Internet, ensure Internet access and Internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the Internet are developed in a secure manner and that they comply with well-established Internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under the [Directive XXX/XXXX (NIS2)] by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products.

(12) Regulation (EU) 2017/745 of the European Parliament and of the Council[7] lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament

[7] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

and of the Council[8] lays down rules on *in vitro* diagnostic medical devices. Both Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole life cycle approach are also covered by those Regulations. These requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including *in vitro* diagnostic devices, with guidance on how to fulfil all the relevant essential requirements of Annex I to those Regulations with regard to cybersecurity.[9] Products with digital elements to which either of those Regulations apply should therefore not be subject to this Regulation.

(13) Regulation (EU) 2019/2144 of the European Parliament and of the Council[10] establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire lifecycle of vehicles, equipment and services in compliance with the applicable United Nations regulations on technical specifications and cybersecurity[11], and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council[12] is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats. Products with digital elements to which Regulation (EU) 2019/2144 applies and those products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential

---

8 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

9 MDCG 2019-16, endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745.

10 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (*OJ L 325, 16.12.2019, p. 1)*.

11 UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management system [2021/387].

12 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

requirements and conformity assessment procedures set out in this Regulation., The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation.

(14) This Regulation lays down horizontal cybersecurity rules which are not specific to sectors or certain products with digital elements. Nevertheless, sectoral or product-specific Union rules could be introduced, laying down requirements that address all or some of the risks covered by the essential requirements laid down by this Regulation. In such cases, the application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I of this Regulation may be limited or excluded where such limitation or exclusion is consistent with the overall regulatory framework applying to those products and where the sectoral rules achieve the same level of protection as the one provided for by this Regulation. The Commission is empowered to adopt delegated acts to amend this Regulation by identifying such products and rules. For existing Union legislation where such limitations or exclusions should apply, this Regulation contains specific provisions to clarify its relation with that Union legislation.

(15) Delegated Regulation (EU) 2022/30 specifies that the essential requirements set out in Article 3(3), point (d) (network harm and misuse of network resources), point (e) (personal data and privacy) and point (f) (fraud) of Directive 2014/53/EU apply to certain radio equipment. [Commission implementation decision XXX/2022 on a standardisation request to the European Standardisation Organisations] lays down requirements for the development of specific standards further specifying how these three essential requirements should be addressed. The essential requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU. Further, the essential requirements laid down in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, if the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation.

(16) Directive 85/374/EEC[13] is complementary to this Regulation. That Directive sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault ('strict liability'). Where such a lack of safety consists in a lack of security updates after placing the product on the market, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such security updates should be laid down in this Regulation.

[13] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.85).

(17) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council[14], including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board (EDPB) established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and the Union data protection law should also be created in the area of market surveillance and enforcement. To this end, national market surveillance authorities appointed under this Regulation should cooperate with authorities supervising Union data protection law. The latter should also have access to information relevant for accomplishing their tasks.

(18) To the extent that their products fall within the scope of this Regulation, issuers of European Digital Identity Wallets as referred to in Article [Article 6a(2) of Regulation (EU) No 910/2014, as amended by Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity], should comply with both the horizontal essential requirements established by this Regulation and the specific security requirements established by Article [Article 6a of Regulation (EU) No 910/2014, as amended by Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity]. In order to facilitate compliance, wallet issuers should be able to demonstrate the compliance of European Digital Identity Wallets with the requirements set out respectively in both acts by certifying their products under a European cybersecurity certification scheme established under Regulation (EU) 2019/881 and for which the Commission specified via implementing act a presumption of conformity for this Regulation, in so far as the certificate, or parts thereof, covers those requirements.

(19) Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it gathers, ENISA should prepare a biennial technical report on

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1).

emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [Directive XXX / XXXX (NIS2)]. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised. In exceptional circumstances, at the request of the Commission, ENISA should be able to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.

(20) Products with digital elements should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.

(21) In order to ensure that manufacturers can release software for testing purposes before subjecting their products to conformity assessment, Member States should not prevent the making available of unfinished software, such as alpha versions, beta versions or release candidates, as long as the version is only made available for the time necessary to test it and gather feedback. Manufacturers should ensure that software made available under these conditions is only released following a risk assessment and that it complies to the extent possible with the security requirements relating to the properties of products with digital elements imposed by this Regulation. Manufacturers should also implement the vulnerability handling requirements to the extent possible. Manufacturers should not force users to upgrade to versions only released for testing purposes.

(22) In order to ensure that products with digital elements, when placed on the market, do not pose cybersecurity risks to persons and organisations, essential requirements should be set out for such products. When the products are subsequently modified, by physical or digital means, in a way that is not foreseen by the manufacturer and that may imply that they no longer meet the relevant essential requirements, the modification should be considered as substantial. For example, software updates or repairs could be assimilated to maintenance operations provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended use for which the product has been assessed may be changed. As is the case for physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.

(23) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, whenever a substantial modification occurs that may affect the compliance of a product with this Regulation or when the intended purpose of that product changes, it is appropriate that the compliance of the product with digital elements is verified and that, where applicable, it undergoes a new conformity assessment. Where applicable, if the manufacturer undertakes a conformity

assessment involving a third party, changes that might lead to substantial modifications should be notified to the third party.

(24) Refurbishing, maintaining and repairing of a product with digital elements, as defined in the Regulation [Eco-design Regulation], does not necessarily lead to a substantial modification of the product, for instance if the intended use and functionalities are not changed and the level of risk remains unaffected. However, upgrading a product by the manufacturer might lead to changes in the design and development of the product and therefore might affect the intended use and the compliance of the product with the requirements set out in this Regulation.

(25) Products with digital elements should be considered critical if the negative impact of the exploitation of potential cybersecurity vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality, or the intended use. In particular, vulnerabilities in products with digital elements that have a cybersecurity-related functionality, such as secure elements, can lead to a propagation of security issues throughout the supply chain. The severity of the impact of a cybersecurity incident may also increase when taking into account the intended use of the product, such as in an industrial setting or in the context of an essential entity of the type referred to in Annex [Annex I] to Directive [Directive XXX/ XXXX (NIS2)], or for the performance of critical or sensitive functions, such as processing of personal data.

(26) Critical products with digital elements should be subject to stricter conformity assessment procedures, while keeping a proportionate approach. For this purpose, critical products with digital elements should be divided into two classes, reflecting the level of cybersecurity risk linked to these categories of products. A potential cyber incident involving products in class II might lead to greater negative impacts than an incident involving products in class I, for instance due to the nature of their cybersecurity-related function or intended use in sensitive environments, and therefore should undergo a stricter conformity assessment procedure.

(27) The categories of critical products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation lists products which are defined by their core functionality as general purpose microprocessors in class II. As a result, general purpose microprocessors are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a general purpose microprocessor. The Commission should adopt delegated acts [by 12 months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III.

(28) This Regulation addresses cybersecurity risks in a targeted manner. Products with digital elements might, however, pose other safety risks, that are not related to cybersecurity. Those risks should continue to be regulated by other relevant Union product legislation. If no other Union harmonisation legislation is applicable, they should be subject to Regulation [General Product Safety Regulation]. Therefore, in light of the targeted nature of this Regulation, as a derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] should apply to products with digital elements with respect to safety risks not covered by this Regulation, if those products are not subject to

specific requirements imposed by other Union harmonisation legislation within the meaning of [Article 3, point (25) of the General Product Safety Regulation].

(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation[15] [the AI Regulation] which fall within the scope of this Regulation should comply with the essential requirements set out in this Regulation. When those high-risk AI systems fulfil the essential requirements of this Regulation, they should be deemed compliant with the cybersecurity requirements set out in Article [Article 15] of Regulation [the AI Regulation] in so far as those requirements are covered by the EU declaration of conformity or parts thereof issued under this Regulation. As regards the conformity assessment procedures relating to the essential cybersecurity requirements of a product with digital elements covered by this Regulation and classified as a high-risk AI system, the relevant provisions of Article 43 of Regulation [the AI Regulation] should apply as a rule instead of the respective provisions of this Regulation. However, this rule should not result in reducing the necessary level of assurance for critical products with digital elements covered by this Regulation. Therefore, by way of derogation from this rule, high-risk AI systems that fall within the scope of the Regulation [the AI Regulation] and are also qualified as critical products with digital elements pursuant to this Regulation and to which the conformity assessment procedure based on internal control referred to in Annex VI of the Regulation [the AI Regulation] applies, should be subject to the conformity assessment provisions of this Regulation in so far as the essential requirements of this Regulation are concerned. In this case, for all the other aspects covered by Regulation [the AI Regulation] the respective provisions on conformity assessment based on internal control set out in Annex VI to Regulation [the AI Regulation] should apply.

(30) The machinery products falling within the scope of Regulation [Machinery Regulation proposal] which are products with digital elements within the meaning of this Regulation and for which a declaration of conformity has been issued on the basis of this Regulation should be deemed to be in conformity with the essential health and safety requirements set out in [Annex III, sections 1.1.9 and 1.2.1] of the Regulation [Machinery Regulation proposal], as regards protection against corruption and safety and reliability of control systems in so far as the compliance with those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.

(31) Regulation [European Health Data Space Regulation proposal] complements the essential requirements laid down in this Regulation. The electronic health record systems ('EHR systems') falling under the scope of Regulation [European Health Data Space Regulation proposal] which are products with digital elements within the meaning of this Regulation should therefore also comply with the essential requirements set out in this Regulation. Their manufacturers should demonstrate conformity as required by Regulation [European Health Data Space Regulation proposal]. To facilitate compliance, manufacturers may draw up a single technical documentation containing the elements required by both legal acts. As this Regulation does not cover SaaS as such, EHR systems offered through the SaaS licensing and delivery model are not within the scope of this Regulation. Similarly, EHR systems that are developed and used in-house are not within the scope of this Regulation, as they are not placed on the market.

(32) In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as throughout their life-cycle, it is necessary to lay

[15] Regulation [the AI Regulation].

down essential requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential requirements related to vulnerability handling and ensure that all their products are delivered without any known exploitable vulnerabilities, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product. For this purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential requirements and in order to appropriately apply suitable harmonised standards or common specifications.

(33) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential requirements. These essential requirements should be without prejudice to the EU coordinated risk assessments of critical supply chains established by [Article X] of Directive [Directive XXX/XXXX(NIS2)][16], which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, it should be without prejudice to the Member States' prerogatives to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Recommendation (EU) 2019/534, in the Union-wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the NIS Cooperation Group as referred to in [Directive XXX/XXXX (NIS2)].

(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of Directive [Directive XX/XXXX (NIS2)] are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database.

(35) Manufacturers should also report to ENISA any incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive [Directive XXX/XXXX (NIS2)] for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the

[16] Directive XXX of the European Parliament and of the Council of [date] [on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ L xx, date, p.x)].

manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.

(36) Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities. A coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, manufacturers of such products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts (so-called 'bug bounty programmes').

(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties.

(38) In order to facilitate assessment of conformity with the requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements which are in conformity with harmonised standards, which translate the essential requirements of this Regulation into detailed technical specifications, and which are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council[17]. Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements of this Regulation.

(39) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, processes and services. European cybersecurity certification schemes can cover products with digital elements covered by this Regulation. This Regulation should create synergies with Regulation (EU) 2019/881. In order to facilitate the assessment of conformity with the requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and which has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity certification schemes for products with digital elements should be assessed in the light of this Regulation. Such future European cybersecurity

[17] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

certification schemes covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation. The Commission should be empowered to specify, by means of implementing acts, the European cybersecurity certification schemes that can be used to demonstrate conformity with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, where applicable, the Commission should specify if a cybersecurity certificate issued under such European cybersecurity certification schemes eliminates the obligation for manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements.

(40) Upon entry into force of the implementing act setting out the [Commission Implementing Regulation (EU) No …/... of XXX on the European Common Criteria-based cybersecurity certification scheme] (EUCC) which concerns hardware products covered by this Regulation, such as hardware security modules and microprocessors, the Commission may specify, by means of an implementing act, how the EUCC provides a presumption of conformity with the essential requirements as referred to in Annex I of this Regulation or parts thereof. Furthermore, such implementing act may specify how a certificate issued under the EUCC eliminates the obligation for manufacturers to carry out a third-party assessment as requested by this Regulation for corresponding requirements.

(41) Where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation request by any of the European standardisation organisations, undue delays in the establishment of appropriate harmonised standards, or a lack of compliance of developed standards with the requirements of this Regulation or with a request of the Commission. In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.

(42) Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential requirements of this Regulation and, where applicable, of the other relevant Union harmonisation legislation by which the product is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legislation. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.

(43) The CE marking, indicating the conformity of a product, is the visible consequence of a whole process comprising conformity assessment in a broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of

the European Parliament and of the Council[18]. Rules governing the affixing of the CE marking on products with digital elements should be laid down in this Regulation. The CE marking should be the only marking which guarantees that products with digital elements comply with the requirements of this Regulation.

(44) In order to allow economic operators to demonstrate conformity with the essential requirements laid down in this Regulation and to allow market surveillance authorities to ensure that products with digital elements made available on the market comply with these requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council[19] establishes modules for conformity assessment procedures in proportion to the level of risk involved and the level of security required. In order to ensure inter-sectoral coherence and to avoid ad-hoc variants, conformity assessment procedures adequate for verifying the conformity of products with digital elements with the essential requirements set out in this Regulation have been based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole life cycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product.

(45) As a general rule the conformity assessment of products with digital elements should be carried out by the manufacturer under its own responsibility following the procedure based on Module A of Decision 768/2008/EC. The manufacturer should retain flexibility to choose a stricter conformity assessment procedure involving a third-party. If the product is classified as a critical product of class I, additional assurance is required to demonstrate conformity with the essential requirements set out in this Regulation. The manufacturer should apply harmonised standards, common specifications or cybersecurity certification schemes under Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act, if it wants to carry out the conformity assessment under its own responsibility (module A). If the manufacturer does not apply such harmonised standards, common specifications or cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party. Taking into account the administrative burden on manufacturers and the fact that cybersecurity plays an important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures respectively based on modules B+C or module H of Decision 768/2008/EC have been chosen as most appropriate for assessing the compliance of critical products with digital elements in a proportionate and effective manner. The manufacturer that carries out the third-party conformity assessment can choose the procedure that suits best its design and production process. Given the even greater cybersecurity risk linked with the use of products classified as critical class II products, the conformity assessment should always involve a third party.

(46) While the creation of tangible products with digital elements usually requires manufacturers to make substantial efforts throughout the design, development and production phases, the creation of products with digital elements in the form of

---

[18] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

[19] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

software almost exclusively focuses on design and development, while the production phase plays a minor role. Nonetheless, in many cases software products still need to be compiled, built, packaged, made available for download or copied onto physical media before being placed on the market. These activities should be considered as activities amounting to production when applying the relevant conformity assessment modules to verify the compliance of the product with the essential requirements of this Regulation across the design, development and production phases.

(47) In order to carry out third-party conformity assessment for products with digital elements, conformity assessment bodies should be notified by the national notifying authorities to the Commission and the other Member States, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.

(48) In order to ensure a consistent level of quality in the performance of conformity assessment of products with digital elements, it is also necessary to lay down requirements for notifying authorities and other bodies involved in the assessment, notification and monitoring of notified bodies. The system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008. Since accreditation is an essential means of verifying the competence of conformity assessment bodies, it should also be used for the purposes of notification.

(49) Transparent accreditation as provided for in Regulation (EC) No 765/2008, ensuring the necessary level of confidence in certificates of conformity, should be considered by the national public authorities throughout the Union as the preferred means of demonstrating the technical competence of conformity assessment bodies. However, national authorities may consider that they possess the appropriate means of carrying out that evaluation themselves. In such cases, in order to ensure the appropriate level of credibility of evaluations carried out by other national authorities, they should provide the Commission and the other Member States with the necessary documentary evidence demonstrating the compliance of the conformity assessment bodies evaluated with the relevant regulatory requirements.

(50) Conformity assessment bodies frequently subcontract parts of their activities linked to the assessment of conformity or have recourse to a subsidiary. In order to safeguard the level of protection required for the product with digital elements to be placed on the market, it is essential that conformity assessment subcontractors and subsidiaries fulfil the same requirements as notified bodies in relation to the performance of conformity assessment tasks.

(51) The notification of a conformity assessment body should be sent by the notifying authority to the Commission and the other Member States via the New Approach Notified and Designated Organisations (NANDO) information system. NANDO is the electronic notification tool developed and managed by the Commission where a list of all notified bodies can be found.

(52) Since notified bodies may offer their services throughout the Union, it is appropriate to give the other Member States and the Commission the opportunity to raise objections concerning a notified body. It is therefore important to provide for a period during which any doubts or concerns as to the competence of conformity assessment bodies can be clarified before they start operating as notified bodies.

(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic

operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.

(54) Market surveillance is an essential instrument in ensuring the proper and uniform application of Union legislation. It is therefore appropriate to put in place a legal framework within which market surveillance can be carried out in an appropriate manner. Rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 of the European Parliament and of the Council[20] apply to products with digital elements covered by this Regulation.

(55) In accordance with Regulation (EU) 2019/1020, market surveillance authorities carry out market surveillance in the territory of that Member State. This Regulation should not prevent Member States from choosing the competent authorities to carry out those tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States may choose to designate any existing or new authority to act as market surveillance authority, including national competent authorities referred to in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] or designated national cybersecurity certification authorities referred to in Article 58 of Regulation (EU) 2019/881. Economic operators should fully cooperate with market surveillance authorities and other competent authorities. Each Member State should inform the Commission and the other Member States of its market surveillance authorities and the areas of competence of each of those authorities and should ensure the necessary resources and skills to carry out the surveillance tasks relating to this Regulation. As per Article 10(2) and (3) of Regulation (EU) 2019/1020, each Member State should appoint a single liaison office that should be responsible, among others, for representing the coordinated position of the market surveillance authorities and assisting in the cooperation between market surveillance authorities in different Member States.

(56) A dedicated administrative cooperation group (ADCO) should be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. This ADCO should be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of the single liaison offices. The Commission should support and encourage cooperation between market surveillance authorities through the Union Product Compliance Network, established on the basis of Article 29 of Regulation (EU) 2019/1020 and comprising representatives from each Member State, including a representative of each single liaison office referred to in Article 10 of Regulation (EU) 2019/1020 and an optional national expert, the chairs of ADCOs, and representatives from the Commission. The Commission should participate in the meetings of the Network, its sub-groups and this respective ADCO. It should also assist this ADCO by means of an executive secretariat that provides technical and logistic support.

(57) In order to ensure timely, proportionate and effective measures in relation to products with digital elements presenting a significant cybersecurity risk, a Union safeguard procedure should be foreseen under which interested parties are informed of measures

[20] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

intended to be taken with regard to such products. This should also allow market surveillance authorities, in cooperation with the relevant economic operators, to act at an earlier stage where necessary. Where the Member States and the Commission agree as to the justification of a measure taken by a Member State, no further involvement of the Commission should be required, except where non-compliance can be attributed to shortcomings of a harmonised standard.

(58) In certain cases, a product with digital elements which complies with this Regulation, may nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in [Annex I to Directive XXX/XXXX (NIS2)] or to other aspects of public interest protection. Therefore it is necessary to establish rules which ensure mitigation of those risks. As a result, market surveillance authorities should take measures to require the economic operator to ensure that the product no longer presents that risk, to recall it or to withdraw it, depending on the risk. As soon as a market surveillance authority restricts or forbids the free movement of a product in such way, the Member State should notify without delay the Commission and the other Member States of the provisional measures, indicating the reasons and justification for the decision. Where a market surveillance authority adopts such measures against products presenting a risk, the Commission should enter into consultation with the Member States and the relevant economic operator or operators without delay and should evaluate the national measure. On the basis of the results of this evaluation, the Commission should decide whether the national measure is justified or not. The Commission should address its decision to all Member States and immediately communicate it to them and the relevant economic operator or operators. If the measure is considered justified, the Commission may also consider adopting proposals to revise the respective Union legislation.

(59) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that these are not compliant with this Regulation, or for products that are compliant with this Regulation, but that present other important risks, such as risks to the health or safety of persons, fundamental rights or the provision of the services by essential entities of the type referred to in [Annex I of Directive XXX / XXXX (NIS2)], the Commission may request ENISA to carry out an evaluation. Based on that evaluation, the Commission may adopt, through implementing acts, corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling of the respective products, within a reasonable period, commensurate with the nature of the risk. The Commission may have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the good functioning of the internal market, and only where no effective measures have been taken by surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities under the scope of [Directive XXX / XXXX (NIS2)], while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the non-compliance with this Regulation or the important risks presented persist.

(60) In cases where there are indications of non-compliance with this Regulation in several Member States, market surveillance authorities should be able to carry out joint activities with other authorities, with a view to verifying compliance and identifying cybersecurity risks of products with digital elements.

(61) Simultaneous coordinated control actions ('sweeps') are specific enforcement actions by market surveillance authorities that can further enhance product security. Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps could be organised to the market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives.

(62) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission in respect of updates to the list of critical products in Annex III and specifying the definitions of the these product categories. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential mandating of certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[21]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to: specify the format and elements of the software bill of materials, specify further the type of information, format and procedure of the notifications on actively exploited vulnerabilities and incidents submitted to ENISA by the manufacturers, 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 therefore as set out in Annex I of this Regulation, adopt common specifications in respect of the essential requirements set out in Annex I, 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, decide on corrective or restrictive measures at Union level in exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market. Those

[21] OJ L 123, 12.5.2016, p. 1.

powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[22].

(64) In order to ensure trustful and constructive cooperation of market surveillance authorities at Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.

(65) In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. Maximum levels for administrative fines to be provided for in national laws for non-compliance with the obligations laid down in this Regulation should therefore be established. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation should be taken into account and as a minimum those explicitly established in this Regulation, including whether administrative fines have been already applied by other market surveillance authorities to the same operator for similar infringements. Such circumstances can be either aggravating, in situations where the infringement by the same operator persists on the territory of other Member States than the one where an administrative fine has already been applied, or mitigating, in ensuring that any other administrative fine considered by another market surveillance authority for the same economic operator or the same type of breach should already take account, along with other relevant specific circumstances, of a penalty and the quantum thereof imposed in other Member States. In all such cases, the cumulative administrative fine that could be applied by market surveillance authorities of several Member States to the same economic operator for the same type of infringement should ensure the respect of the principle of proportionality.

(66) Where administrative fines are imposed on persons that are not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines.

(67) In its relationships with third countries, the EU endeavours to promote international trade in regulated products. A broad variety of measures can be applied in order to facilitate trade, including several legal instruments such as bilateral (inter-governmental) Mutual Recognition Agreements (MRAs) for conformity assessment and marking of regulated products. MRAs are established between the Union and third countries, which are on a comparable level of technical development and have a compatible approach concerning conformity assessment. These agreements are based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party. Currently MRAs are in place for several countries. The agreements are concluded in a number of specific sectors, which might vary from one country to another. In order to further facilitate trade, and recognising that supply chains of products with digital elements are global, MRAs concerning conformity assessment may be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU. Cooperation with partner countries is also

[22] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

important, in order to strengthen cyber resilience globally, as in the long term this will contribute to a strengthened cybersecurity framework both within and outside of the EU.

(68) The Commission should periodically review this Regulation, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

(69) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. This Regulation should apply [24 months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [12 months] from the entry into force of this Regulation.

(70) Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(71) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[23] and delivered its opinion on […],

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This Regulation lays down:

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

(b) 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;

(c) 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;

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

[23] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Article 2

Scope

1. This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

2. This Regulation does not apply to products with digital elements to which the following Union acts apply:

   (a) Regulation (EU) 2017/745;

   (b) Regulation (EU) 2017/746;

   (c) Regulation (EU) 2019/2144.

3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.

4. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:

   (a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and

   (b) the sectoral rules achieve the same level of protection as the one provided for by this Regulation.

   The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend this Regulation specifying whether such limitation or exclusion is necessary, the concerned products and rules, as well as the scope of the limitation, if relevant.

5. This Regulation does not apply to products with digital elements developed exclusively for national security or military purposes or to products specifically designed to process classified information.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) ‘product with digital elements’ means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately;

(2) ‘remote data processing’ means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

(3) ‘critical product with digital elements’ means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III;

(4) ‘highly critical product with digital elements’ means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(5);

(5) ‘operational technology’ means programmable digital systems or devices that interact with the physical environment or manage devices that interact with the physical environment;

(6) ‘software’ means the part of an electronic information system which consists of computer code;

(7) ‘hardware’ means a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data;

(8) ‘component’ means software or hardware intended for integration into an electronic information system;

(9) ‘electronic information system’ means any system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;

(10) ‘logical connection’ means a virtual representation of a data connection implemented through a software interface;

(11) ‘physical connection’ means any connection between electronic information systems or components implemented using physical means, including through electrical or mechanical interfaces, wires or radio waves;

(12) ‘indirect connection’ means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network;

(13) ‘privilege’ means an access right granted to particular users or programmes to perform security-relevant operations within an electronic information system;

(14) ‘elevated privilege’ means an access right granted to particular users or programmes to perform an extended set of security-relevant operations within an electronic information system that, if misused or compromised, could allow a malicious actor to gain wider access to the resources of a system or organisation;

(15) ‘endpoint’ means any device that is connected to a network and serves as an entry point to that network;

(16) ‘networking or computing resources’ means data or hardware or software functionality that is accessible either locally or through a network or another connected device;

(17) ‘economic operator’ means the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations laid down by this Regulation;

(18) ‘manufacturer’ means any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment or free of charge;

(19) ‘authorised representative’ means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his or her behalf in relation to specified tasks;

(20) ‘importer’ means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union;

(21) ‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties;

(22) ‘placing on the market’ means the first making available of a product with digital elements on the Union market;

(23) ‘making available on the market’ means any supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(24) ‘intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

(25) ‘reasonably foreseeable use’ means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions;

(26) ‘reasonably foreseeable misuse’ means the use of a product with digital elements in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;

(27) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;

(28) ‘conformity assessment’ means the process of verifying whether the essential requirements set out in Annex I have been fulfilled;

(29) ‘conformity assessment body’ means a body defined in Article 2(13) of Regulation (EU) No 765/2008;

(30) ‘notified body’ means a conformity assessment body designated in accordance with Article 33 of this Regulation and other relevant Union harmonisation legislation;

(31) ‘substantial modification’ means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed;

(32) ‘CE marking’ means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential requirements set out in Annex I and other applicable Union legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;

(33) ‘market surveillance authority’ means the authority as defined in Article 3, point (4) of Regulation (EU) 2019/1020;

(34) ‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012;

(35) ‘cybersecurity risk’ means risk as defined in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)];

(36) ‘significant cybersecurity risk’ means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;

(37) ‘software bill of materials’ means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;

(38) ‘vulnerability’ means a vulnerability as defined in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)];

(39) ‘actively exploited vulnerability’ means a vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner;

(40) ‘personal data’ means data as defined in Article 4(1) of Regulation (EU) 2016/679.

Article 4

Free movement

1. Member States shall not impede, for the matters covered by this Regulation, the making available on the market of products with digital elements which comply with this Regulation.

2. At trade fairs, exhibitions and demonstrations or similar events, Member States shall not prevent the presentation and use of a product with digital elements which does not comply with this Regulation.

3. Member States shall not prevent the making available of unfinished software which does not comply with this Regulation provided that the software is only made available for a limited period required for testing purposes and that a visible sign clearly indicates that it does not comply with this Regulation and will not be available on the market for purposes other than testing.

Article 5

Requirements for products with digital elements

Products with digital elements shall only be made available on the market where:

(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated, and

(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I.

Article 6

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 into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products.

2. The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list of 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 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:

      (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 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 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:

(a) used or relied upon by the essential entities of the type referred to in Annex [Annex I] to the Directive [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 supply chain of products with digital elements against disruptive events.

Article 7

General product safety

By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation] where products with digital elements are not subject to specific requirements laid down in other Union harmonisation legislation within the meaning of [Article 3, point (25) of the General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] shall apply to those products with respect to safety risks not covered by this Regulation.

Article 8

High-risk AI systems

1. Products with digital elements classified as high-risk AI systems in accordance with Article [Article 6] of Regulation [the AI Regulation] which fall within the scope of this Regulation, and fulfil the essential requirements set out in Section 1 of Annex I of this Regulation, and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I, shall be deemed in compliance with the requirements related to cybersecurity set out in Article [Article 15] of Regulation [the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.

2. For the products and cybersecurity requirements referred to in paragraph 1, the relevant conformity assessment procedure as required by Article [Article 43] of Regulation [AI Regulation] shall apply. For the purpose of that assessment, notified bodies which are entitled to control the conformity of the high-risk AI systems under the Regulation [AI Regulation] shall be also entitled to control the conformity of the high-risk AI systems within the scope of this Regulation with the requirements set out in Annex I to this Regulation, provided that the compliance of those notified bodies with the requirements laid down in Article 29 of this Regulation have been assessed in the context of the notification procedure under Regulation [AI Regulation].

3. By derogation from paragraph 2, critical products with digital elements listed in Annex III of this Regulation, which have to apply the conformity assessment procedures referred to in Articles 24(2)(a), 24(2)(b), 24(3)(a) and 24(3)(b) under this Regulation and which are also classified as high-risk AI systems according to Article [Article 6] of the Regulation [AI Regulation] and to which the conformity

assessment procedure based on internal control referred to in Annex [Annex VI] to Regulation [the AI Regulation] applies, shall be subject to the conformity assessment procedures as required by this Regulation in so far as the essential requirements of this Regulation are concerned.

Article 9

Machinery products

Machinery products under the scope of Regulation [Machinery Regulation proposal] which are products with digital elements within the meaning of this Regulation and for which an EU declaration of conformity has been issued on the basis of this Regulation shall be deemed to be in conformity with the essential health and safety requirements set out in Annex [Annex III, Sections 1.1.9 and 1.2.1] to Regulation [Machinery Regulation proposal], as regards protection against corruption and safety and reliability of control systems, and in so far as the achievement of the level of protection required by those requirements is demonstrated in the EU declaration of conformity issued under this Regulation.

CHAPTER II

OBLIGATIONS OF ECONOMIC OPERATORS

Article 10

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.

2. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.

3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.

4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements.

5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities they become aware of and

any relevant information provided by third parties, and, where applicable, update the risk assessment of the product.

6. When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

   Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

7. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23.

   They shall carry out the chosen conformity assessment procedures referred to in Article 24 or have them carried out.

   Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22.

8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.

9. Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.

10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements.

11. Manufacturers shall either provide the EU declaration of conformity with the product with digital elements or include in the instructions and information set out in Annex II the internet address at which the EU declaration of conformity can be accessed.

12. From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall

immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.

13. Manufacturers shall, further to a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by it, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in Annex I. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements, which they have placed on the market.

14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market.

15. The Commission may, by means of implementing acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Article 11

Reporting obligations of manufacturers

1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any actively exploited vulnerability contained in the product with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability.

2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any incident having impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

5. The Commission may, by means of implementing acts, specify further the type of information, format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

6. ENISA, on the basis of the notifications received pursuant to paragraphs 1 and 2, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)]. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.

7. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component.

Article 12

Authorised representatives

1. A manufacturer may appoint an authorised representative by a written mandate.

2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.

3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:

   (a) keep the EU declaration of conformity referred to in Article 20 and the technical documentation referred to in Article 23 at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market;

   (b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;

   (c) cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.

Article 13

Obligations of importers

1. Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.

2. Before placing a product with digital elements on the market, importers shall ensure that:

   (a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer;

   (b) the manufacturer has drawn up the technical documentation;

   (c) the product with digital elements bears the CE marking referred to in Article 22 and is accompanied by the information and instructions for use as set out in Annex II.

3. Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.

4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and the email address at which they can be contacted on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.

5. Importers shall ensure that the product with digital elements is accompanied by the instructions and information set out in Annex II in a language which can be easily understood by users.

6. Importers who know or have reason to believe that a product with digital elements, which they have placed on the market, or the processes put in place by its manufacturer, are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity with the essential requirements set out in Annex I, or to withdraw or recall the product, if appropriate.

   Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

7. Importers shall, for ten years after the product with digital elements has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.

8. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put

in place by the manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.

9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Article 14

Obligations of distributors

1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements of this Regulation.

2. Before making a product with digital elements available on the market, distributors shall verify that:

   (a) the product with digital elements bears the CE marking;

   (b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), 10(11) and 13(4).

3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.

4. Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.

   Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

5. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in

Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market.

6. When the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Article 15

Cases in which obligations of manufacturers apply to importers and distributors

An importer or distributor shall be considered a manufacturer for the purposes of this Regulation and shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7) where that importer or distributor places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements already placed on the market.

Article 16

Other cases in which obligations of manufacturers apply

A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation.

That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.

Article 17

Identification of economic operators

1. Economic operators shall, on request and where the information is available, provide to the market surveillance authorities the following information:

   (a) name and address of any economic operator who has supplied them with a product with digital elements;

   (b) name and address of any economic operator to whom they have supplied a product with digital elements;

2. Economic operators shall be able to present the information referred to in paragraph 1 for ten years after they have been supplied with the product with digital elements and for ten years after they have supplied the product with digital elements.

CHAPTER III

CONFORMITY OF THE PRODUCT WITH DIGITAL ELEMENTS

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 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 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).

Article 19

Common specifications

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.

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.

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 to the 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 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.

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 of the following procedures:

(a) EU-type examination procedure (based on module B) provided for 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.

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 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.

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.

CHAPTER IV

NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

Article 25

Notification

Member States shall notify the Commission and the other Member States of conformity assessment bodies authorised to carry out conformity assessments in accordance with this Regulation.

Article 26

Notifying authorities

1. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, including compliance with Article 31.

2. Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with Regulation (EC) No 765/2008.

Article 27

Requirements relating to notifying authorities

1. A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs.

2. A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities.

3. A notifying authority shall be organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment.

4. A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis.

5. A notifying authority shall safeguard the confidentiality of the information it obtains.

6. A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.

Article 28

Information obligation on notifying authorities

1. Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes thereto.

2. The Commission shall make that information publicly available.

Article 29

Requirements relating to notified bodies

1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12.

2. A conformity assessment body shall be established under national law and have legal personality.

3. A conformity assessment body shall be a third-party body independent of the organisation or the product it assesses.

A body belonging to a business association or professional federation representing undertakings involved in the design, development, production, provision, assembly, use or maintenance of products with digital elements which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered such a body.

4. A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.

A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, development, production, the marketing, installation, use or maintenance of those products, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services.

Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.

6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VI and in relation to which it has been notified, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.

At all times and for each conformity assessment procedure and each kind or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary:

(a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency and the ability of reproduction of those procedures. It shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process.

It shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities.

7. The personnel responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;

(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the essential requirements, of the applicable harmonised standards and of the relevant provisions of Union harmonisation legislation and of its implementing acts;

(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

8. The impartiality of the conformity assessment bodies, their top level management and of the assessment personnel shall be guaranteed.

The remuneration of the top level management and assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.

9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.

10. The personnel of a conformity assessment body shall observe professional secrecy with regard to all information obtained in carrying out their tasks under Annex VI or any provision of national law giving effect to it, except in relation to the market surveillance authorities of the Member State in which its activities are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.

11. Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 40 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group.

12. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, in particular taking into account the interests of SMEs in relation to fees.

Article 30

Presumption of conformity of notified bodies

Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* it shall be presumed to comply with the requirements set out in Article 29 in so far as the applicable harmonised standards cover those requirements.

Article 31

Subsidiaries of and subcontracting by notified bodies

1. Where a notified body subcontracts specific tasks connected with conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 29 and shall inform the notifying authority accordingly.

2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established.

3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the manufacturer.

4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.

Article 32

Application for notification

1. A conformity assessment body shall submit an application for notification to the notifying authority of the Member State in which it is established.

2. That application shall be accompanied by a description of the conformity assessment activities, the conformity assessment procedure or procedures and the product or products for which that body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 29.

3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 29.

Article 33

Notification procedure

1. Notifying authorities may notify only conformity assessment bodies, which have satisfied the requirements laid down in Article 29.

2. The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations (NANDO) information system developed and managed by the Commission.

3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and product or products concerned and the relevant attestation of competence.

4. Where a notification is not based on an accreditation certificate as referred to in Article 32(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 29.

5. The body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification where an accreditation certificate is used or within two months of a notification where accreditation is not used.

   Only such a body shall be considered a notified body for the purposes of this Regulation.

6. The Commission and the other Member States shall be notified of any subsequent relevant changes to the notification.

Article 34

Identification numbers and lists of notified bodies

1. The Commission shall assign an identification number to a notified body.

   It shall assign a single such number even where the body is notified under several Union acts.

2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been allocated to them and the activities for which they have been notified.

   The Commission shall ensure that that list is kept up to date.

Article 35

Changes to notifications

1. Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 29, or that it is failing to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.

2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying Member State shall take appropriate steps to ensure that the files of that body are either processed by another notified body or kept available for the responsible notifying and market surveillance authorities at their request.

Article 36

Challenge of the competence of notified bodies

1. The Commission shall investigate all cases where it doubts, or doubt is brought to its attention regarding the competence of a notified body or the continued fulfilment by a notified body of the requirements and responsibilities to which it is subject.

2. The notifying Member State shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the body concerned.

3. The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated confidentially.

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including de-notification if necessary.

Article 37

Operational obligations of notified bodies

1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 24 and Annex VI.

2. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for economic operators. Conformity assessment bodies shall perform their activities taking due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process.

3. Notified bodies shall however respect the degree of rigour and the level of protection required for the compliance of the product with the provisions of Regulation.

4. Where a notified body finds that requirements laid down in Annex I or in corresponding harmonised standards or in common specifications as referred to in Article 19 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a conformity certificate.

5. Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product no longer complies with the requirements laid down in this Regulation, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the certificate if necessary.

6. Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any certificates, as appropriate.

Article 38

Information obligation on notified bodies

1. Notified bodies shall inform the notifying authority of the following:

   (a) any refusal, restriction, suspension or withdrawal of a certificate;

   (b) any circumstances affecting the scope of and conditions for notification;

   (c) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;

   (d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

2. Notified bodies shall provide the other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same products with relevant information on issues relating to negative and, on request, positive conformity assessment results.

Article 39

Exchange of experience

The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification policy.

Article 40

Coordination of notified bodies

1. The Commission shall ensure that appropriate coordination and cooperation between notified bodies are put in place and properly operated in the form of a cross-sectoral group of notified bodies.
2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

CHAPTER V

MARKET SURVEILLANCE AND ENFORCEMENT

Article 41

Market surveillance and control of products with digital elements in the Union market

1. Regulation (EU) 2019/1020 shall apply to the products with digital elements within the scope of this Regulation.
2. Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation.
3. Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated under Article 58 of Regulation (EU) 2019/881 and exchange information on a regular basis. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 11 of this Regulation, the designated market surveillance authorities shall cooperate with ENISA.
4. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, and exchange information on a regular basis.
5. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing these authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 8 of this Article if such guidance and advice concerns the processing of personal data.

Authorities supervising Union data protection law shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks. They shall inform the designated market surveillance authorities of the Member State concerned of any such request.

6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and human resources to fulfil their tasks under this Regulation.

7. The Commission shall facilitate the exchange of experience between designated market surveillance authorities.

8. Market surveillance authorities may provide guidance and advice to economic operators on the implementation of this Regulation, with the support of the Commission.

9. The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law.

10. For products with digital elements in the scope of this Regulation classified as high-risk AI systems according to Article [Article 6] of the Regulation [the AI Regulation], the market surveillance authorities designated for the purposes of the Regulation [the AI Regulation] shall be the authorities responsible for market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall cooperate, as appropriate, with the market surveillance authorities designated pursuant to this Regulation and, with respect to the supervision of the implementation of the reporting obligations pursuant to Article 11, with ENISA. Market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall in particular inform market surveillance authorities designated pursuant to this Regulation of any finding relevant for the fulfilment of their tasks in relation to the implementation of this Regulation.

11. A dedicated administrative cooperation group (ADCO) shall be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. This ADCO shall be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of single liaison offices.

Article 42

Access to data and documentation

Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the respective economic operator.

Article 43

Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk

1. Where the market surveillance authority of a Member State has sufficient reasons to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall carry out an evaluation of the product with digital elements concerned in respect of its compliance with all the requirements laid down in this Regulation. The relevant economic operators shall cooperate as necessary with the market surveillance authority.

   Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

   The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the appropriate corrective actions.

2. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the operator to take.

3. The manufacturer shall ensure that all appropriate corrective action is taken in respect of all the products with digital elements concerned that it has made available on the market throughout the Union.

4. Where the manufacturer of a product with digital elements does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it.

   That authority shall inform the Commission and the other Member States, without delay, of those measures.

5. The information referred to in paragraph 4 shall include all available details, in particular the data necessary for the identification of the non-compliant products with digital elements, the origin of the product with digital elements, the nature of the alleged non-compliance and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authority shall indicate whether the non-compliance is due to one or more of the following:

   (a) a failure of the product or of the processes put in place by the manufacturer to meet the essential requirements set out in Annex I;

   (b) shortcomings in the harmonised standards, cybersecurity certification schemes, or common specifications, referred to in Article 18.

6. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without

delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product concerned, and, in the event of disagreement with the notified national measure, of their objections.

7. Where, within three months of receipt of the information referred to in paragraph 4, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the operator concerned in accordance with Article 18 of Regulation (EU) 2019/1020.

8. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product concerned, such as withdrawal of the product from their market, without delay.

Article 44

Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 43(4), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union legislation, the Commission shall without delay enter into consultation with the relevant Member State and the economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within nine months from the notification referred to in Article 43(4) and notify such decision to the Member State concerned.

2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant product with digital elements is withdrawn from their market, and shall inform the Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure.

3. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in the harmonised standards, the Commission shall apply the procedure provided for in Article 10 of Regulation (EU) No 1025/2012.

4. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in a European cybersecurity certification scheme as referred to in Article 18, the Commission shall consider whether to amend or repeal the implementing act as referred to in Article 18(4) that specifies the presumption of conformity concerning that certification scheme.

5. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in common specifications as referred to in Article 19, the Commission shall consider whether to amend or repeal the implementing act referred to in Article 19 setting out those common specifications.

Article 45

Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk

1. Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it may request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.

2. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission may request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

3. Based on ENISA's evaluation, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.

4. On the basis of the consultation referred to in paragraph 3, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

5. The Commission shall immediately communicate the decision referred to in paragraph 4 to the relevant economic operator or operators. Member States shall implement the acts referred to in paragraph 4 without delay and shall inform the Commission accordingly.

6. Paragraphs 2 to 5 are applicable for the duration of the exceptional situation that justified the Commission's intervention and for as long as the respective product is not brought in compliance with this Regulation.

Article 46

Compliant products with digital elements which present a significant cybersecurity risk

1. Where, having performed an evaluation under Article 43, the market surveillance authority of a Member State finds that although a product with digital elements and the processes put in place by the manufacturer are in compliance with this Regulation, they present a significant cybersecurity risk and, in addition, they pose a risk to the health or safety of persons, to the compliance with obligations under Union or national law intended to protect fundamental rights, the availability authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in [Annex I to Directive XXX / XXXX (NIS2)] or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that the

product with digital elements and the processes put in place by the manufacturer concerned, when placed on the market, no longer present that risk, to withdraw the product with digital elements from the market or to recall it within a reasonable period, commensurate with the nature of the risk.

2. The manufacturer or other relevant operators shall ensure that corrective action is taken in respect of the products with digital elements concerned that they have made available on the market throughout the Union within the timeline established by the market surveillance authority of the Member State referred to in paragraph 1.

3. The Member State shall immediately inform the Commission and the other Member States about the measures taken pursuant to paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the products with digital elements concerned, the origin and the supply chain of those products with digital elements, the nature of the risk involved and the nature and duration of the national measures taken.

4. The Commission shall without delay enter into consultation with the Member States and the relevant economic operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.

5. The Commission shall address its decision to the Member States.

6. Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements, although compliant with this Regulation, presents the risks referred to in paragraph 1, it may request the relevant market surveillance authority or authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43 and paragraphs 1, 2 and 3 of this Article.

7. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product referred to in paragraph 6 continues to present the risks referred to in paragraph 1 and no effective measures have been taken by the relevant national market surveillance authorities, the Commission may request ENISA to carry out an evaluation of the risks presented by that product and shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

8. Based on ENISA's evaluation referred to in paragraph 7, the Commission may establish that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant operator or operators.

9. On the basis of the consultation referred to in paragraph 8, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

10. The Commission shall immediately communicate the decision referred to in the paragraph 9 to the relevant operator or operators. Member States shall implement such acts without delay and shall inform the Commission accordingly.

11. Paragraphs 6 to 10 shall apply for the duration of the exceptional situation that justified the Commission's intervention and for as long as the respective product continues to present the risks referred to in paragraph 1.

Article 47

Formal non-compliance

1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant manufacturer to end to the non-compliance concerned:

   (a) the conformity marking has been affixed in violation of Articles 21 and 22;

   (b) the conformity marking has not been affixed;

   (c) the EU declaration of conformity has not been drawn up;

   (d) the EU declaration of conformity has not been drawn up correctly;

   (e) the identification number of the notified body, which is involved in the conformity assessment procedure, where applicable, has not been affixed;

   (f) the technical documentation is either not available or not complete.

2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product with digital elements from being made available on the market or ensure that it is recalled or withdrawn from the market.

Article 48

Joint activities of market surveillance authorities

1. Market surveillance authorities may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks.

2. The Commission or ENISA may propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products falling in the scope of this Regulation with the requirements laid down by the latter.

3. The market surveillance authorities and the Commission, where applicable, shall ensure that the agreement to carry out joint activities does not lead to unfair competition between economic operators and does not negatively affect the objectivity, independence and impartiality of the parties to the agreement.

4. A market surveillance authority may use any information resulting from the activities carried out as part of any investigation that it undertakes.

5. The market surveillance authority concerned and the Commission, where applicable, shall make the agreement on joint activities, including the names of the parties involved, available to the public.

Article 49

Sweeps

1. Market surveillance authorities may decide to conduct simultaneous coordinated control actions ("sweeps") of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation.

2. Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep may, where appropriate, make the aggregated results publicly available.

3. ENISA may identify, in the performance of its tasks, including based on the notifications received according to Article 11(1) and (2), categories of products for which sweeps may be organised. The proposal for sweeps shall be submitted to the potential coordinator referred to in paragraph 2 for the consideration of the market surveillance authorities.

4. When conducting sweeps, the market surveillance authorities involved may use the investigation powers set out Articles 41 to 47 and any other powers conferred upon them by national law.

5. Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.

CHAPTER VI

DELEGATED POWERS AND COMMITTEE PROCEDURE

Article 50

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) shall be conferred on the Commission.

3. The delegation of power referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) shall enter into force only if no objection has

been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 51

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.

CHAPTER VII

CONFIDENTIALITY AND PENALTIES

Article 52

Confidentiality

1. All parties involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

   (a) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive 2016/943 of the European Parliament and of the Council[24];

   (b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;

   (c) public and national security interests;

   (d) integrity of criminal or administrative proceedings.

2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the market surveillance authorities and between market surveillance authorities and the Commission shall not be disclosed without the prior agreement of the originating market surveillance authority.

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and

[24] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law of the Member States.

4. The Commission and Member States may exchange, where necessary, sensitive information with relevant authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of protection.

Article 53

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements by economic operators of this Regulation and shall take all measures necessary to ensure that they are enforced. The penalties provided for shall be effective, proportionate and dissuasive.

2. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.

3. The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

   (a) the nature, gravity and duration of the infringement and of its consequences;

   (b) whether administrative fines have been already applied by other market surveillance authorities to the same operator for a similar infringement;

   (c) the size and market share of the operator committing the infringement.

7. Market surveillance authorities that apply administrative fines shall share this information with the market surveillance authorities of other Member States through the information and communication system referred to in Article 34 of Regulation (EU) 2019/1020.

8. Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

9. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or other bodies according to the competences established at national level in those Member States. The application of such rules in those Member States shall have an equivalent effect.

10. Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement.

CHAPTER VIII

TRANSITIONAL AND FINAL PROVISIONS

Article 54

Amendment to Regulation (EU) 2019/1020

In Annex I to Regulation (EU) 2019/1020 the following point is added:
’71. [Regulation XXX][Cyber Resilience Act]’.

Article 55

Transitional provisions

1. EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for products with digital elements that are subject to other Union harmonisation legislation shall remain valid until [42 months after the date of entry into force of this Regulation], unless they expire before that date, or unless otherwise specified in other Union legislation, in which case they shall remain valid as referred to in that Union legislation.

2. Products with digital elements that have been placed on the market before [date of application of this Regulation referred to in Article 57], shall be subject to requirements of this Regulation only if, from that date, those products are subject to substantial modifications in their design or intended purpose.

3. By way of derogation from paragraph 2, the obligations laid down in Article 11 shall apply to all products with digital elements within the scope of this Regulation that have been placed on the market before [date of application of this Regulation referred to in Article 57].

Article 56

Evaluation and review

By [36 months after the date of application of this Regulation] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

Article 57

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [24 months after the date of entry into force of this Regulation]. However Article 11 shall apply from [12 months after the date of entry into force of this Regulation].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5. Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

3.2.2. Estimated output funded with operational appropriations

3.2.3. Summary of estimated impact on administrative appropriations

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)

1.2. Policy area(s) concerned

Communications Networks, Content and Technology

1.3. The proposal/initiative relates to:

× **a new action**

☐ **a new action following a pilot project/preparatory action**[37]

☐ **the extension of an existing action**

☐ **a merger or redirection of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

The proposal has two main objectives aiming to ensure the proper functioning of the internal market: (1) **create conditions for the development of secure products with digital elements** by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle; and (2) **create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements**.

1.4.2. Specific objective(s)

Four specific objectives were set out for the proposal: (i) to ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle; (ii) to ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers; (iii) to enhance the transparency of security properties of products with digital elements, and (iv) to enable businesses and consumers to use products with digital elements securely.

Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The proposal would bring significant benefits to the various stakeholders. For businesses, it would prevent divergent security rules for products with digital elements and decrease compliance costs for related cybersecurity legislation. It would reduce the number of cyber incidents, incident handling costs and reputational damage. For the whole EU, it is estimated that the initiative could lead to a costs reduction from incidents affecting companies by approximately EUR 180 billion to

[37] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

EUR 290 billion annually[38]. It would lead to an increased turnover due to uptake of products with digital elements demand. It would improve the companies' global reputation leading to a demand uptake also outside the EU. For users, the preferred option would enhance the transparency of the security properties and facilitate the use of products with digital elements. Consumers and citizens would also benefit from better protection of their fundamental rights, such as privacy and data protection.

At the same time, the proposal would add compliance and enforcement costs for businesses, notified bodies and public authorities, including accreditation and market surveillance authorities. For software developers and hardware manufacturers, it will add direct compliance costs for new security requirements, conformity assessment, documentation and reporting obligations, leading to aggregated compliance costs amounting to up to roughly EUR 29 billion for an estimated market value of EUR 1485 billion in turnover[39]. Users, including business users, consumers and citizens may face higher prices of products with digital elements. However, they should be seen against the background of the significant benefits as described above.

1.4.3. Indicators of performance

Specify the indicators for monitoring progress and achievements.

In order to test if manufacturers improve the security of their products with digital elements since the design and development phase and throughout the whole life cycle of those products, several indicators could be taken into account. These could be the number of significant incidents in the Union caused by vulnerabilities, the share of hardware and software manufacturers that follow a systematic secure development life cycle, a qualitative analysis of the security of products with digital elements, a quantitative and qualitative assessment of vulnerability databases, the frequency of security patches made available by manufacturers or the average number of days between vulnerability discovery and the provision of security patches.

An indicator for a coherent cybersecurity framework could be the absence of targeted product-specific national cybersecurity legislation.

An indicator for an enhanced transparency regarding the security properties of products with digital elements could be the share of products with digital elements that are shipped with information on security properties. Moreover, the share of products with digital elements that are shipped with user instructions on secure use could be used as an indicator whether organisations and consumers are being enabled to use products with digital elements securely.

As regards the monitoring of the impact of the regulation, certain indicators would be considered for this purpose, to be assessed by the Commission, where appropriate with the support of ENISA. Depending on the operational objective to be reached, some of the monitoring indicators based on which the success of the horizontal cybersecurity requirements would be assessed are as follows:

For assessing the level of cybersecurity of products with digital elements:

[38] See [Commission Staff Working Document on Impact Assessment Report accompanying the Regulation on horizontal cybersecurity requirements for products with digital elements]

[39] See [Commission Staff Working Document on Impact Assessment Report accompanying the Regulation on horizontal cybersecurity requirements for products with digital elements]

- Statistics and qualitative analysis on incidents affecting products with digital elements and the way these were handled. These could be gathered and assessed by the Commission, with support from ENISA.

- Records of known vulnerabilities and analyses of how these were handled. Such analysis could be conducted by ENISA, based on the European vulnerability database set up based on [Directive XXX/ XXXX (NIS2)].

- Surveys amongst manufacturers of hardware and software to monitor progress.

For assessing the level of information on security features, security support, end-of-life and duty of care: results of surveys to be conducted by the Commission, with support from ENISA for both users and businesses.

For assessing the implementation, the Commission would aim to ensure that the conformity assessments are effectively performed. To this end, a standardization request will be issued and its implementation followed. The Commission will also verify the capacity of the notified bodies and, if applicable, of the certification bodies.

As regards the application, by means of the reports of Member States, the Commission will verify that national initiatives do not concern aspects covered by the regulation.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The Regulation should be fully applicable 24 months after its entry into force. However, elements of the governance structure should be in place before then. In particular, Member States shall have appointed existing authorities and/or established new authorities performing the tasks set out in the legislation.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

The strong cross-border nature of cybersecurity and the growing incidents with spill-over effects across borders, sectors and products, mean that the objectives cannot effectively be achieved by Member States alone. Given the global nature of product with digital elements markets, Member States face the same risks for the same product with digital elements on their territory. An emerging patchy framework of potentially diverging national rules also risks hampering an open and competitive single market for products with digital elements. Joint action at EU level is thus necessary to increase the level of trust among users and the attractiveness of EU products with digital elements. It would also benefit the internal market by providing legal certainty and achieving a level playing field for vendors of products with digital elements.

1.5.3. Lessons learned from similar experiences in the past

The Cyber Resilience Act is the first regulation of its kind, introducing cybersecurity requierements for the placement on the market of products with digital elements. It builds however on the setting of the New Legislative Framework and the lessons learnt in the implementation process of existing Union harmonisation legislation of a variety of products, notably as regards the preparation for implementation, including aspects such as preparation of harmonised standards.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The Regulation on horizontal cybersecurity requirements for products with digital elements defines new cybersecurity requirements for all products with digital elements placed on the EU market, going beyond any requirements provided by existing legislation. At the same time, the proposal is building on the existing setting of the NLF legislation. Therefore, it would build on existing NLF structures and procedures such as the cooperation of notified bodies and market surveillance, conformity assessment modules, development of harmonised standards. The new proposal would also rely on some structures developed according to other cybersecurity legislation such as the Directive 2016/1148 (NIS Directive), respectively the [Directive XXX/ XXXX (NIS2)], or Regulation 2019/881 (the Cybersecurity Act).

1.5.5. Assessment of the different available financing options, including scope for redeployment

The management of the action areas assigned to ENISA fits its existing mandate and general tasks. These action areas may require specific profiles or new assignments, but these would not be notable and can be absorbed by the existing resources of ENISA and resolved through reallocation or linking of various assignments. For example, one of the main action areas assigned to ENISA concerns the gathering and processing of notifications from manufacturers on exploited product vulnerabilities. [Directive XXX/ XXXX (NIS2)] has already tasked ENISA to establish a European vulnerability database where publicly known vulnerabilities can be disclosed and registered, on a voluntary basis, for the purpose of allowing users to take appropriate mitigating measures. Resources allocated for that purpose could also be used for the new above-mentioned assignments relating to notifications of product vulnerabilities. That could ensure an effective use of existing resources and would also create the necessary synergies between such assignments that can better inform ENISA’s analyses of cybersecurity risks and threats.

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

× **unlimited duration**

– Implementation with a start-up period from 2025.

– followed by full-scale operation.

1.7. Management mode(s) planned[40]

☐ **Direct management** by the Commission

– × by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

This Regulation assigns certain actions to ENISA, in line with its existing mandate, and in particular Art 3(2) of Regulation 2019/881 establishing that ENISA should carry out the tasks assigned to it by Union legal acts that set out measures for approximating Member State laws, regulations and administrative provisions which are related to cybersecurity. In particular, ENISA is tasked to receive notifications from manufacturers of actively exploited vulnerabilities contained in the products with digital elements, as well as incidents having an impact on the security of these products. ENISA should also forward these notifications to the relevant CSIRTs or, respectively, to the relevant single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States, as well as inform the market surveillance authorities. Based on the

[40] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the NIS Cooperation Group. Furthermore, considering ENISA's expertise, information gathered and threat analyses, ENISA may support the implementation process of this Regulation by proposing joint activities to be conducted by national market surveillance authorities based on indications or information of potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions may be organised. ENISA may be requested by the Commission to conduct evaluations for specific products in exceptional circumstances in relation to products with digital elements that present a significant cybersecurity risk and where an immediate intervention is required to preserve the good functioning of the internal market.
All these assignments are estimated to about 4.5 FTEs from the existing resources of ENISA, building already on expertise and preparatory work that it is currently done by ENISA, among others in support of the upcoming implementation of [Directive XXX/ XXXX (NIS2)] for which ENISA's resources were supplemented.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

By 36 months after the date of application of this Regulation and every four years thereafter, the Commission will submit a report on its evaluation and review to the European Parliament and to the Council. The reports shall be made public.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

This Regulation establishes a new policy with regard to harmonised cybersecurity requirements for products with digital elements placed on the internal market throughour their whole life cycle. The legal act will be followed by requests by the Commission to the European standardisation bodies to develop standards.

In order to face these new tasks, it is necessary to appropriately resource the Commission's services. The enforcement of the new Regulation is estimated to require 7 FTEs (of which one END) to cover the following tasks:

- Preparation of the standardisation request and/or common specifications via implementing acts absent successful standardisation process;
- Preparing a delegated act [within 12 months since the entry into force of the Regulation] specifying the definitions of the critical products with digital elements;
- Potential preparation of delegated acts for updating the list of critical products of class I and II; specifying whether a limitation or exclusion is necessary for products with digital elements covered by other Union rules laying down requirements achieving the same level of protection as this Regulation; mandating the certification of certain highly critical products with digital elements based on criteria set out in this Regulation; specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation;
- Potential preparation of implementing acts relating to the format or elements of the reporting obligations, software bill of materials, common specifications or affixing of CE marking;
- Potentially preparing an immediate intervention for imposing corrective or restrictive measures in exceptional circumstances to preserve the good functioning of the internal market, including the preparation of an implementing act;
- Organisation and coordination of the notifications by Member States of notified bodies and coordination of the Notified Bodies;
- Supporting the coordination of Member States' market surveillance authorities.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

In order to ensure that notified bodies and market surveillance authorities exchange information and cooperate well, the Commission is in charge of their coordination. For the technical and market expertise, an expert group would be created.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. For the meeting expenditures, given the low value per transaction (e.g. refunding travel costs for a delegate for a meeting), standard control procedures seem sufficient. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

The existing fraud prevention measures applicable to the Commission will cover the additional appropriations necessary for this Regulation.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

Schema

- New budget lines requested

N/A

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☑ The proposal/initiative does not require the use of operational appropriations

– ☐ The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	

DG: <…….>			Year **N**[41]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
• Operational appropriations										
Budget line[42]	Commitments	(1a)								
	Payments	(2a)								
Budget line	Commitments	(1b)								
	Payments	(2b)								
Appropriations of an administrative nature financed from the envelope of specific programmes[43]										
Budget line		(3)								
TOTAL appropriations for DG <…….>	Commitments	=1a+1b +3								
	Payments	=2a+2b +3								

• TOTAL operational appropriations	Commitments	(4)								
	Payments	(5)								

41 Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

42 According to the official budget nomenclature.

43 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADING <….> of the multiannual financial framework	Commitments	=4+ 6								
	Payments	=5+ 6								

If more than one operational heading is affected by the proposal / initiative, repeat the section above:

• TOTAL operational appropriations (all operational headings)	Commitments	(4)								
	Payments	(5)								
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings)		(6)								
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6								
	Payments	=5+ 6								

Heading of multiannual financial framework	7	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year 2024	Year 2025	Year 2026	Year 2027	TOTAL
DG: CNECT						
• Human resources		1.030	1.030	1.030	1.030	**4.120**
• Other administrative expenditure		**0.222**	**0.222**	**0.222**	**0.222**	**0.888**
TOTAL DG CNECT	Appropriations	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**

EUR million (to three decimal places)

		Year 2024	Year 2025	Year 2026	Year 2027	TOTAL
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**
	Payments	**1.252**	**1.252**	**1.252**	**1.252**	**5.008**

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year N	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)	TOTAL
	OUTPUTS							

⇩	Type [44]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[45]…																				
- Output																				
- Output																				
- Output																				
Subtotal for specific objective No 1																				
SPECIFIC OBJECTIVE No 2 ...																				
- Output																				
Subtotal for specific objective No 2																				
TOTALS																				

[44] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

[45] As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. Summary of estimated impact on administrative appropriations

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2024**	Year **2025**	Year **2026**	Year **2027**	
HEADING 7 of the multiannual financial framework					
Human resources	1.030	1.030	1.030	1.030	**4.120**
Other administrative expenditure	0.222	0.222	0.222	0.222	**0.888**
Subtotal HEADING 7 of the multiannual financial framework	1.252	1.252	1.252	1.252	**5.008**
Outside HEADING 7[46] of the multiannual financial framework					
Human resources					
Other expenditure of an administrative nature					
Subtotal outside HEADING 7 of the multiannual financial framework					
TOTAL	1.252	1.252	1.252	1.252	**5.008**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

[46] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.3.1. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources.

– ☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		Year **2024**	Year **2025**	Year **2026**	Year **2027**
20 01 02 01 (Headquarters and Commission's Representation Offices)		6	6	6	6
20 01 02 03 (Delegations)					
01 01 01 01 (Indirect research)					
01 01 01 11 (Direct research)					
Other budget lines (specify)					
• External staff (in Full Time Equivalent unit: FTE)[47]					
20 02 01 (AC, END, INT from the 'global envelope')		1	1	1	1
20 02 03 (AC, AL, END, INT and JPD in the delegations)					
XX 01 xx **yy zz** [48]	- at Headquarters				
	- in Delegations				
01 01 01 02 (AC, END, INT - Indirect research)					
01 01 01 12 (AC, END, INT - Direct research)					
Other budget lines (specify)					
TOTAL		**7**	**7**	**7**	**7**

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff 6 FTEs x 157.000 €/ year = € 942.000	As described under 2.2.1: – Preparation of the standardisation request and/or common specifications via implementing acts absent successful standardisation process; – Preparing a delegated act [within 12 months since the entry into force of the Regulation] specifying the definitions of the critical products with digital elements; – Potential preparation of delegated acts for updating the list of critical products of class I and II; specifying whether a limitation or exclusion is necessary for products with digital elements covered by other Union rules laying down requirements achieving the same level of protection as this Regulation; mandating the certification of certain highly critical products with digital elements based on criteria set out in this Regulation; specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation; – Potential preparation of implementing acts relating to the format or elements of the reporting obligations, software bill of materials, common

[47] AC= Contract Staff; AL = Local Staff; END= Seconded National Expert; INT = agency staff; JPD= Junior Professionals in Delegations.

[48] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

	specifications or affixing of CE marking; – Potentially preparing an immediate intervention for imposing corrective or restrictive measures in exceptional circumstances to preserve the good functioning of the internal market, including the preparation of an implementing act; – Organisation and coordination of the notifications by Member States of notified bodies and coordination of the Notified Bodies; – Supporting the coordination of Member States' market surveillance authorities.
External staff 1 END x 88.000 €/ year	As described under 2.2.1: – Preparation of the standardisation request and/or common specifications via implementing acts absent successful standardisation process; – Preparing a delegated act [within 12 months since the entry into force of the Regulation] specifying the definitions of the critical products with digital elements; – Potential preparation of delegated acts for updating the list of critical products of class I and II; specifying whether a limitation or exclusion is necessary for products with digital elements covered by other Union rules laying down requirements achieving the same level of protection as this Regulation; mandating the certification of certain highly critical products with digital elements based on criteria set out in this Regulation; specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation; – Potential preparation of implementing acts relating to the format or elements of the reporting obligations, software bill of materials, common specifications or affixing of CE marking; – Potentially preparing an immediate intervention for imposing corrective or restrictive measures in exceptional circumstances to preserve the good functioning of the internal market, including the preparation of an implementing act; – Organisation and coordination of the notifications by Member States of notified bodies and coordination of the Notified Bodies; – Supporting the coordination of Member States' market surveillance authorities.

3.2.4. Compatibility with the current multiannual financial framework

The proposal/initiative:

– x can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

No reprogramming is required.

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

-

– ☐ requires a revision of the MFF.

-

3.2.5. Third-party contributions

The proposal/initiative:

– x does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **N**[49]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[49] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

3.3. Estimated impact on revenue

– ☐ The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

– ☐ on own resources

– ☐ on other revenue

– please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[50]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[50] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454

ANNEXES 1 to 6

ANNEXES

to the

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

{SEC(2022) 321} - {SWD(2022) 282} - {SWD(2022) 283}

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

1. Security requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product (‘minimisation of data’);

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

2. Vulnerability handling requirements

Manufacturers of the products with digital elements shall:

(4) 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;

(5) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

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

(7) once a security update has been made available, publically 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 information helping users to remediate the vulnerabilities;

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

(9) 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;

(10) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(11) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

ANNEX II

INFORMATION AND INSTRUCTIONS TO THE USER

As a minimum, the product with digital elements shall be accompanied by:

1. the name, registered trade name or registered trade mark of the manufacturer, and the postal address and the email address at which the manufacturer can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product;
2. the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;
3. the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;
4. the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;
5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;
6. if and, where applicable, where the software bill of materials can be accessed;
7. where applicable, the internet address at which the EU declaration of conformity can be accessed;
8. the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates;
9. detailed instructions or an internet address referring to such detailed instructions and information on:
   (a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;
   (b) how changes to the product can affect the security of data;
   (c) how security-relevant updates can be installed;
   (d) the secure decommissioning of the product, including information on how user data can be securely removed.

ANNEX III

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class I

10. Identity management systems software and privileged access management software;
11. Standalone and embedded browsers;
12. Password managers;
13. Software that searches for, removes, or quarantines malicious software;
14. Products with digital elements with the function of virtual private network (VPN);
15. Network management systems;
16. Network configuration management tools;
17. Network traffic monitoring systems;
18. Management of network resources;
19. Security information and event management (SIEM) systems;
20. Update/patch management, including boot managers;
21. Application configuration management systems;
22. Remote access/sharing software;
23. Mobile device management software;
24. Physical network interfaces;
25. Operating systems not covered by class II;
26. Firewalls, intrusion detection and/or prevention systems not covered by class II;
27. Routers, modems intended for the connection to the internet, and switches, not covered by class II;
28. Microprocessors not covered by class II;
29. Microcontrollers;
30. 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)];
31. 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);
32. Industrial Internet of Things not covered by class II.

Class II

33. Operating systems for servers, desktops, and mobile devices;

34. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;

35. Public key infrastructure and digital certificate issuers;

36. Firewalls, intrusion detection and/or prevention systems intended for industrial use;

37. General purpose microprocessors;

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

39. Routers, modems intended for the connection to the internet, and switches, intended for industrial use;

40. Secure elements;

41. Hardware Security Modules (HSMs);

42. Secure cryptoprocessors;

43. Smartcards, smartcard readers and tokens;

44. Industrial Automation & Control Systems (IACS) 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);

45. 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)];

46. Robot sensing and actuator components and robot controllers;

47. Smart meters.

ANNEX IV

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 20, shall contain all of the following information:

48. Name and type and any additional information enabling the unique identification of the product with digital elements;

49. Name and address of the manufacturer or his authorised representative;

50. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;

51. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);

52. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;

53. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;

54. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;

55. Additional information:

Signed for and on behalf of: ……

(place and date of issue):

(name, function) (signature):

ANNEX V

CONTENTS OF THE TECHNICAL DOCUMENTATION

The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements:

56. a general description of the product with digital elements, including:

    (e) its intended purpose;

    (f) versions of software affecting compliance with essential requirements;

    (g) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;

    (h) user information and instructions as set out in Annex II;

57. a description of the design, development and production of the product and vulnerability handling processes, including:

    (i) complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;

    (j) complete information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;

    (k) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.

58. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation;

59. a list of the harmonised standards applied in full or in part the references of which have been published in the *Official Journal of the European Union*, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied;

60. reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;

61. a copy of the EU declaration of conformity;

62. where applicable, the software bill of materials as defined in Article 3, point (36), further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I.

ANNEX VI

CONFORMITY ASSESSMENT PROCEDURES

Conformity Assessment procedure based on internal control (based on Module A)

63. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I.

64. The manufacturer shall draw up the technical documentation described in Annex V.

65. Design, development, production and vulnerability handling of products with digital elements

The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I.

66. Conformity marking and declaration of conformity

66.1. The manufacturer shall affix the CE to each individual product with digital elements that satisfies the applicable requirements of this Regulation.

66.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

67. Authorised representatives

The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.

EU-type examination (based on Module B)

68. EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I.

69. EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product through examination of the

technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type).

70. The manufacturer shall lodge an application for EU-type examination with a single notified body of his choice.

The application shall include:

– the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;

– a written declaration that the same application has not been lodged with any other notified body;

– the technical documentation, which shall make it possible to assess the product's conformity with the applicable essential requirements as set out in Section 1 of Annex I and the manufacturer's vulnerability handling processes set out in Section 2 of Annex I, and shall include an adequate analysis and assessment of the risk(s). The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex V;

– the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards and/or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under his responsibility.

71. The notified body shall:

71.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with the essential requirements set out in Section 1 of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I;

71.2. verify that the specimen(s) have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards and/or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;

71.3. carry out appropriate examinations and tests, or have them carried out, to check whether, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I, these have been applied correctly;

71.4. carry out appropriate examinations and tests, or have them carried out, to check whether, where the solutions in the relevant harmonised standards and/or technical

specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential requirements;

71.5. agree with the manufacturer on a location where the examinations and tests will be carried out.

72. The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.

73. Where the type and the vulnerability handling processes meet the essential requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes. The certificate may have one or more annexes attached.

The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.

Where the type and the vulnerability handling processes do not satisfy the applicable essential requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.

74. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.

The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.

75. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued.

The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and/or additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.

76. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market.

77. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 9, provided that they are specified in the mandate.

Conformity to type based on internal production control (based on Module C)

78. Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 3, and ensures and declares that the products concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential requirements set out in Section 1 of Annex I.

79. Production

79.1. The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with the approved type described in the EU-type examination certificate and with the essential requirements as set out in Section 1 of Annex I.

80. Conformity marking and declaration of conformity

80.1. The manufacturer shall affix the CE marking to each individual product that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements of the legislative instrument.

80.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

81. Authorised representative

The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.

Conformity based on full quality assurance (based on Module H)

82. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5, and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of

Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I.

83. Design, development, production and vulnerability handling of products with digital elements

The manufacturer shall operate an approved quality system as specified in point 3 for the design, development, and production of the products concerned and for handling vulnerabilities, maintain its effectiveness throughout the lifecycle of the products concerned, and shall be subject to surveillance as specified in point 4.

84. Quality system

84.1. The manufacturer shall lodge an application for assessment of his quality system with the notified body of his choice, for the products concerned.

The application shall include:

– the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;

– the technical documentation for one model of each category of products intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in Annex V;

– the documentation concerning the quality system; and

– a written declaration that the same application has not been lodged with any other notified body.

84.2. The quality system shall ensure compliance of the products with the essential requirements set out in Section 1 of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Section 2 of Annex I.

All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.

It shall, in particular, contain an adequate description of:

– the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;

– the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 1 of Annex I that apply to the products will be met;

– the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 2 of Annex I that apply to the manufacturer will be met;

– the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products pertaining to the product category covered;

– the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;

– the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;

– the quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc;

– the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.

84.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.

It shall presume conformity with those requirements in respect of the elements of the quality system that comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification.

In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and knowledge of the applicable requirements of this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1, second indent, to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with those requirements.

The manufacturer or his authorised representative shall be notified of the decision.

The notification shall contain the conclusions of the audit and the reasoned assessment decision.

84.4. The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.

84.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system.

The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.

85. Surveillance under the responsibility of the notified body

85.1. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.

85.2. The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:

– the quality system documentation;

– the quality records as provided for by the design part of the quality system, such as results of analyses, calculations, tests, etc.;

– the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.

85.3. The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.

86. Conformity marking and declaration of conformity

86.1. The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product that satisfies the requirements set out in Section 1 of Annex I to this Regulation.

86.2. The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up.

A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

87. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market, keep at the disposal of the national authorities:

– the technical documentation referred to in point 3.1;

– the documentation concerning the quality system referred to in point 3.1;

– the change referred to in point 3.5, as approved;

– the decisions and reports of the notified body referred to in points 3.5, 4.3 and 4.4.

88. Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.

89. Authorised representative

The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.

General Information Note Template

The standardised note format/font/numbering layout should be used for all information notes submitted with the exception of Green/White papers (see Annex II) or pre-adoption confidential CFSP draft measures:

Font type:	Times New Roman
Font size:	12
Page Layout:	Portrait, single column format
Format:	Word (*.doc) or Rich Text Format (*.rtf) (Not *.docx)

The information to be inserted is noted in italics under each heading.

Information Note

1. Proposal
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

2. Date of Commission document
15/09/2022

3. Number of Commission document
COM (2022) 454 Final

4. Number of Council document:
2022/0272 (COD)

5. Dealt with in Brussels by
Telecommunications Council / Horizontal Working Party on Cyber Issues

6. Department with primary responsibility
Department of the Environment, Climate and Communications

7. Other Departments involved
Department of Enterprise, Trade and Employment

8. Background to, short summary and aim of the proposal
Background to Proposal
This proposal builds on the EU's New Legislative Framework and the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).
The Commission's proposal highlights that many products offered for sale in the Single Market have a low level of cyber security, and also that consumers do not have the necessary information to make informed choices when seeking to purchase devices which are cyber secure. The cybersecurity of products with digital elements has a strong cross-border dimension, as products manufactured in one country are often used across the internal

market. In addition, incidents initially affecting a single entity or a single Member State often spread within minutes across the entire internal market. While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs. The proposal refers to a number of recent cyber security incidents impacting in different Member States in which the level of cyber security of digital products was a contributing factor, as well as the cross-border nature of cyber security incidents and threats. The proposal also recalls the forthcoming revised Network and Information Security (NIS2) Directive which will require a large number of entities operating in a broad range of services and industry sectors to implement cyber security risk assessments and to take appropriate technical and organisational measures to prevent and mitigate cyber security incidents on their systems and networks. The relatively low level of cyber security of some digital products sold in the EU markets and of the information available to inform purchasing decisions hampers these entities in identifying and mitigating cyber security risks.

Aim of Proposal

The principal aim of the proposal is to harmonise cybersecurity requirements for products with digital elements in all Member States and to remove obstacles to the free movement of goods. The current EU legislative framework applicable to products with digital elements is based on Article 114 TFEU, and comprises several pieces of legislation, including on specific products and safety-related aspects or general legislation on product liability. However, it covers only certain aspects linked to the cybersecurity of tangible digital products and, as applicable, software embedded in these products. The proposal notes that, at national level, Member States are starting to take national measures requiring vendors of digital products to enhance their cybersecurity.

The Commission is concerned that the various acts and initiatives taken so far at EU and national levels only partially address the problems identified and risk creating a legislative patchwork within the internal market, increasing legal uncertainty for both vendors and users of these products and adding unnecessary burden on companies to comply with a number of requirements for similar types of products.

The proposed Regulation would harmonise and streamline the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements and avoid overlapping requirements stemming from different pieces of legislation. This would create greater legal certainty for operators and users across the Union, as well as a better harmonisation of the European single market, creating more viable conditions for operators aiming at entering the EU market.

Summary of Proposal

This proposed Regulation lays down (a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products; (b) 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; (c) 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; (d) rules on market surveillance and enforcement of the above-mentioned rules and requirements. The proposed Regulation will apply to all products with digital elements whose intended and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

Critical products with digital elements shall be subject to specific conformity assessment procedures and shall be divided into class I and class II as set out in an annex to the proposal, reflecting their cybersecurity risk level, with class II representing a greater risk. A product with digital elements is considered critical and therefore included in the annex taking into account the impact of potential cybersecurity vulnerabilities included in the product with digital elements. The cybersecurity-related functionality of the product with digital elements and the intended use in sensitive environments such as an industrial setting, amongst others, is also considered in the determination of cybersecurity risk. The Commission is also empowered to adopt delegated acts 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 under a European cybersecurity certification scheme to demonstrate conformity with the essential requirements set out in the Regulation.

The proposal incorporates obligations for manufacturers, importers and distributors based on the reference provisions foreseen in Decision 768/2008/EC. The essential cybersecurity requirements and obligations mandate that all products with digital elements shall only be made available on the market if, where duly supplied, properly installed, maintained and used for their intended purpose or under conditions, which can be reasonably foreseen, they meet the essential cybersecurity requirements set out in this proposed Regulation.

In accordance with Regulation (EU) 2019/1020, it is proposed that national market surveillance authorities carry out market surveillance in the territory of that Member State. Economic operators are asked to fully cooperate with market surveillance authorities and other competent authorities.

9. Legal basis of the proposal

The legal basis for this proposal is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides for the adoption of measures to ensure the establishing and functioning of the internal market. Article 114 TFEU may be used as a legal basis to prevent the occurrence of these obstacles resulting from diverging national laws and approaches on how to address the legal uncertainties and gaps in the existing legal frameworks. Furthermore, the Court of Justice has recognised that applying heterogeneous technical requirements could be valid grounds to trigger Article 114 TFEU. The Regulation is aligned with the New Legislative Framework and per its title builds upon and amends the existing Market Surveillance Regulation (EU) 2019/1020.

10. Voting Method

QMV

11. Role of the EP

Co-Decision

12. Category of proposal
Significant

13. Implications for Ireland & Ireland's Initial View
The proposal will require Ireland to expand its existing regulatory regime for product standards to ensure relevant products are compliant with the standards for cyber security to be set out in the legislation. Ireland will also be required to designate a market surveillance authority for these products. Ireland's initial view is supportive of the measure as it aligns with Government policy on cyber security.

14. Impact on the public?
Enhanced cyber security of products with digital elements available on the European market will reduce the risk of cyber crime, personal data theft and other harms to individuals and businesses. The Regulation may lead to restrictions on the availability of certain products and choice for consumers.

15. Have consultations with Stakeholders taken place or are there any plans to do so?
The Commission has consulted a broad range of stakeholders. Member States and stakeholders were invited to participate in the open public consultation and in the surveys and workshops organised in the context of a study conducted by a consortium supporting the Commission's preparatory work for the impact assessment: Wavestone, the Centre for European Policy Studies (CEPS) and ICF. The consulted stakeholders included national market surveillance authorities, Union bodies dealing with cybersecurity, hardware and software manufacturers, importers and distributors of hardware and software, trade associations, consumer organisations and users of products with digital elements and citizens, researchers and academia, notified bodies and accreditation bodies, and cybersecurity industry professionals.

Consultation activities included:
- *A first study conducted by a consortium consisting of ICF, Wavestone, Carsa and CEPS, which was published in December 202111. The study identified several market failures and assessed possible regulatory interventions.*
- *An Open Public Consultation that targeted citizens, stakeholders and cybersecurity experts. 176 replies were submitted. These contributed to the collection of diverse opinions and experiences from all stakeholder groups.*
- *Workshops organised by the study supporting the Commission's preparatory work for a Cyber Resilience Act gathered around 100 representatives from all 27 Member States representing a variety of stakeholders.*
- *Expert interviews were conducted to gain a deeper understanding of current cybersecurity challenges related to products with digital elements, and to discuss policy options for a potential regulatory intervention.*
- *Bilateral discussions were held with national cybersecurity authorities, the private sector, and consumer organisations.*
- *Targeted outreach was done to key SME stakeholders.*

16. Are there any subsidiarity issues for Ireland?
Ireland does not currently operate any regulatory regime for the cyber security of products with digital elements. Ireland is establishing a European Cyber Security Certification Authority in the National Cyber Security Centre – as required under the European Cyber

Security Act (Regulation 2019/881) – to oversee a national certification regime for the cyber security certification schemes to be introduced pursuant to Implementing Acts under this regulation. The Regulation provides for voluntary certification schemes to cover products, services and processes however the Council has not yet enacted any relevant Implementing Acts. As referenced above, this proposal may require suppliers of specified categories of critical products to obtain certification for their products under the relevant schemes.

17. Anticipated negotiating period
12-18 months

18. Proposed implementation date
Q3 2023

19. Consequences for national legislation
Supplementing of existing product standards and market surveillance legislation to take account of provisions in this proposal.

20. Method of Transposition into Irish law
Regulation becomes directly applicable upon signature – no transposition required

21. Anticipated Transposition date
See above

22. Consequences for the EU budget in Euros annually
€5,008,000

23. Contact name, telephone number and e-mail address of official in Department with primary responsibility?
Peter Hogan, 0879739846, Peter.Hogan@decc.gov.ie

13 October 2022