

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

([COM\(2022\)0454](#) – C9-0308/2022 – [2022/0272\(COD\)](#))

(Ordinary legislative procedure: first reading)

The European Parliament,

- having regard to the Commission proposal to Parliament and the Council ([COM\(2022\)0454](#)),
- having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0308/2022),
- having regard to Article 294(3) of the Treaty on the Functioning of the European Union,
- having regard to the opinion of the European Economic and Social Committee of 14 December 2022^[1],
- having regard to Rule 59 of its Rules of Procedure,
- having regard to the opinion of the Committee on the Internal Market and Consumer Protection,
- having regard to the report of the Committee on Industry, Research and Energy (A9-0253/2023),

1. Adopts its position at first reading hereinafter set out;
2. Requests the Commission to modify the financial statement accompanying the proposal by increasing the establishment plan of the European Union Agency for Cybersecurity (ENISA) by 9.0 additional full-time posts and by providing corresponding additional appropriations in order to ensure that the obligations of ENISA under this Regulation can be fulfilled and not to compromise existing obligations of the Agency under other Union legislation;
3. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

4. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

Amendment 1

AMENDMENTS BY THE EUROPEAN PARLIAMENT^[*]

to the Commission 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 and Directive 2020/1828/EC (Cyber Resilience Act)

(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^[2],

Having regard to the opinion of the Committee of the Regions^[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) *Cybersecurity is one of the key challenges for the Union and the number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not just on the Union's economy, but also on democracy and consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address cyber resilience at Union level and 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 manufacturers 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, ***for example by improving transparency with regard to the support period of products placed on the market.***
- (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 Regulation (EU) 2019/881 of the European Parliament and of the Council^[4] and ***Directive (EU) 2022/2555 of the European Parliament and of the Council***^[5] does not directly cover mandatory requirements for the security of products with digital elements.
- (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 ***undertakings and organisations*** 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, ***to ensure a harmonised and clear regulatory framework for undertakings, particularly micro, small and medium-sized enterprises.*** 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 ***and proportionality for microenterprises and small and***

medium-sized enterprises, creating more viable conditions for economic operators aiming at entering the Union market.

(4a) The horizontal nature of this Regulation means that it will have an impact on very different segments of the Union's economy. It is therefore important that the specificities of each sector are taken into account and that the cybersecurity requirements laid down in this Regulation are proportional to the risks. The Commission should therefore issue guidelines which explain in a clear and detailed manner how to apply this Regulation. Guidelines should cover inter alia a detailed explanation of the scope, in particular the notion of remote data processing and the implications for free and open-source developers, the criteria used to determine how critical products with digital elements are classified and the interplay between this Regulation and other Union law.

(4b) A business operating online may offer a variety of different services. Depending on the nature of services provided, the same entity may fall under several different categories of economic operators. Where an entity provides online intermediation services for a product with digital elements and is a provider of an online marketplace, as defined in Article 3(14) of Regulation 2023/988 of the European Parliament and of the Council^[6], it does not qualify as an economic operator as defined in this Regulation. Where the same entity is a provider of an online marketplace and acts as an economic operator as defined in this Regulation, for the sale of products with digital elements, it should be subject to the scope of this Regulation with regard to such products. The provisions of Regulation (EU) 2023/988 is fully applicable to this Regulation. Given the prominent role that online marketplaces have in enabling electronic commerce, they should strive to cooperate with the market surveillance authorities of the Member States in order to ensure that products purchased through online marketplaces comply with the cybersecurity requirements laid down in this Regulation.

(5) At Union level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade^[7], the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021^[8], 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^[9], citizens called for "a stronger role for the EU in countering cybersecurity threats". In order for the Union to play a leading international role in the field of cybersecurity, it is important to establish an ambitious overarching regulatory framework.

(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.
- (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. ***Those requirements will also ensure that cybersecurity is taken into account throughout supply chains, making final products with digital elements more secure. This will, in turn, represent a competitive advantage for manufacturers established or represented in the Union, which will be able to advertise the cybersecurity of their products.***
- (9) This Regulation ensures a high level of cybersecurity of products with digital elements ***and their integrated remote data processing solutions. Such*** remote data processing solutions relating to a product with digital elements ***are defined*** as any data processing at a distance for which the software is designed and developed by ***or on behalf of*** the manufacturer of the product concerned ***■***, and the absence of which would prevent such a product with digital elements from performing one of its functions. ***For example, cloud enabled functionalities provided by the manufacturer of smart home devices that enable users to control the device at a distance, should fall within the scope of this Regulation. On the other hand, websites not inextricably linked to a product with digital elements or cloud services outside the responsibility of the manufacturer should not to be considered to be remote data processing solutions under this Regulation. Directive (EU) 2022/2555*** 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. *While Directive (EU) 2022/2555 applies to cloud computing services and cloud service models, and this Regulation does not apply to services, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS), they may fall within the scope of this Regulation to the extent they meet the definition of remote data processing solutions.* ■

- (9a) Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. Research by the European Commission^[10] also shows that free and open-source software can contribute between EUR 65 billion to EUR 95 billion to the Union's GDP and that it can provide significant growth opportunities for the Union's economy. Users are allowed to run, copy, distribute, study, change and improve software and data, including models by way of free and open-source licences. To foster the development and deployment of free and open-source software, in particular by microenterprises and small, medium-sized enterprises, including start-ups, and not-for-profit organisations, academic research and individuals, this Regulation should apply to free and open-source software products in specific cases, to take into account the fact that different development models of software distributed and developed under public licences exist.*
- (10) Only free and open-source software made available on the market in the course of a commercial activity should ■ be covered by this Regulation. ■ Whether a free and open-source product has been made available as part of a commercial activity should be assessed on a product-by-product basis, looking at both the development model and the supply phase of the free and open-source product with digital elements.*
- (10a) For example, a fully decentralised development model, where no single commercial entity exercises control over what is accepted into the project's code base, should be taken as an indication that the product has been developed in a non-commercial setting. On the other hand, where free and open-source software is developed by a single organisation or an asymmetric community, where a single organisation is generating revenues from related use in business relationships, this should be considered to be a commercial activity. Similarly, where the main contributors to free and open-source projects are developers employed by commercial entities and when such developers or the employer can exercise control as to which modifications are accepted in the code base, the project should generally be considered to be of a commercial nature.*
- (10b) With regard to the supply phase, in the context of free and open-source 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, *when this does not serve only for the recuperation of actual costs*, 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. *Accepting donations without the intention of making a profit should not be considered to be a commercial activity, unless such donations are made by commercial entities and are recurring in nature.*

- (10c) Developers contributing individually to free and open-source projects should not be subject to obligations pursuant to this Regulation.*
- (10d) The sole act of hosting free and open-source software on open repositories does not in itself constitute making available on the market of a product with digital elements. As such, most package managers, code hosting and collaboration platforms should not be considered to be distributors within the meaning of this Regulation.*
- (10e) In order to ensure that the products are designed, developed and produced in accordance with the essential requirements provided for in Annex I, Section 1, manufacturers should exercise due diligence when integrating components sourced from third parties, including in the case of free and open-source software that has not been made available on the market. The appropriate level of due diligence depends on the nature and the level of risk of the component and may include one or more of the following actions: checking if the component already carries the CE mark, checking security up-dates history, verifying if it is free from vulnerabilities registered in the European vulnerability database or other public databases, or carrying out additional security tests. Where, in the exercise of due diligence, the manufacturer of the product identifies a vulnerability in a component, including in a free and open-source component, it should inform the developer of the component, address and remedy the vulnerability, and, where applicable, provide the developer with the applied security fix. Once the manufacturer has placed the product on the market, it should be responsible for ensuring that vulnerabilities are handled throughout the support period, including for free and open-source components integrated into the product with digital elements.*
- (10f) The lack of professional skills in the field of cybersecurity is a key issue to be tackled for the successful application of this Regulation. Particular emphasis should be put on the skills gap for manufacturers, market surveillance authorities and notified bodies. Therefore, in line with the Commission's Communication entitled "Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy')", specific measures both at Union and Member States level should be put in place to assess the state and the evolution of the cybersecurity labour market and synergies for cybersecurity education and training offers also addressing the gender gap*

in the sector, with the aim of establishing a common Union approach to cybersecurity training.

- (11) A secure Internet is indispensable for the functioning of critical infrastructures and for society as a whole. Directive (EU) 2022/2555 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 (EU) 2022/2555 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^[11] lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council^[12] 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^[13], 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. Products with digital elements to which either of those Regulations apply should therefore not be subject to this Regulation.
- (12a) Products with digital elements that are developed exclusively for national security or military purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation. However, Member States are encouraged to ensure the same or higher level of protection for those products as for those falling within the scope of this Regulation.***

- (13) Regulation (EU) 2019/2144 of the European Parliament and of the Council^[14] 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^[15], 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^[16] 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 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.
- (14a) In order to ensure that products made available on the market can be repaired effectively and their durability extended, an exemption should be provided for spare parts. This should be the case both for spare parts that have the purpose of repairing legacy products made available before the date of application of this Regulation as well as for spare parts that have already undergone a conformity assessment procedure pursuant to this Regulation and that are supplied by the same manufacturer.***

(14b) Regulation (EU) 2022/2554 of the European Parliament and of the Council^[17] establishes a number of requirements to ensure the security of network and information systems supporting the business processes of financial entities. The Commission should monitor the implementation of this Regulation in the financial sector, to ensure compatibility and to avoid overlaps for products with digital elements that may also be covered by Regulation (EU) 2022/2554.

(14c) Agricultural and forestry vehicles that fall within the scope of Regulation (EU) 167/2013 of the European Parliament and of the Council^[18] also fall within the scope of this Regulation. Future amendments to Regulation (EU) 167/2013 should avoid regulatory overlaps.

(15) **Commission** Delegated Regulation (EU) 2022/30^[19] 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, *when* the Commission **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. *Where manufacturers comply with this Regulation before its date of application, they should be considered also to comply with Commission Delegated Regulation (EU) 2022/30, until the Commission repeals that Delegated Regulation.*

(16) **Council** Directive 85/374/EEC^[20] 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.

(17) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council^[21], 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.

(18a) When procuring products with digital elements, Member States should give priority to products that have a high level of cybersecurity and an appropriate support period, in order to improve their ability to deal with

cyber threats, as well as to ensure the efficient use of public resources. Furthermore, Member States should ensure that manufacturers remedy vulnerabilities that affect publicly procured products with digital elements as soon as possible and as a matter of urgency where such products have a significant risk profile.

(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 **significant** incidents having an impact on the security of those products. *Vulnerabilities subject to mandatory reporting concern instances where an actor is executing malicious code on a product with digital elements in order to generate a security breach, for example by exploiting weaknesses in identification and authentication functions. Vulnerabilities that are discovered with no malicious intent for purposes of good faith testing, investigation, correction or disclosure to promote the security or safety of the system owner and its users should not be subject to mandatory notifications. A significant incident that has an impact on the security of the product with digital elements concerns a cybersecurity incident that can severely affect the development, production and maintenance processes of the manufacturer and that in turn can significantly impact the security of its products. Such a significant incident could include a situation in which, an attacker has successfully compromised the release channel via which the manufacturer releases security updates to users.*

(19a) 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 (EU) 2022/2555, and inform the relevant market surveillance authorities about the notified vulnerability. *ENISA should ensure that those notifications are received, stored and transmitted via secure channels and that clear protocols are in place with regard to who can access them and the arrangements for their onward transmission. ENISA should ensure the confidentiality of those notifications with particular regard to vulnerabilities for which a security update is not yet available.* On the basis of the 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 Cooperation Group referred to in Directive (EU) 2022/2555. 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 ***visibly, legibly and indelibly*** 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. ***Furthermore, at trade fairs, exhibitions and demonstrations or similar events, Member States should not prevent the presentation and use of a prototype product with digital elements.***

(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 ***in a non-production version*** 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, ***necessary security updates***, software updates or repairs ***such as minor adjustment of the source code that can improve the security, should not be considered to be substantial modifications***, 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. ***This is generally the case for new software versions which aim at improving performance and fixing vulnerabilities. Minor functionality updates, such as visual enhancements, the addition of new languages to the user interface or of a new set of pictograms, should generally not be considered to be substantial modifications.*** 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, *as is generally the case for software revisions. The Commission should issue guidelines on how to determine what constitutes a substantial modification.*

- (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 (EU) 2022/2555, or the performance of critical or sensitive functions, *that have an impact on health, safety or fundamental rights.*
- (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 **high risk** 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 I. 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 6 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. *In order to ensure legal clarity and certainty as well as predictability for stakeholders to comply with this Regulation, amendments to the list in Annex III should be made at the earliest two years after the entry into force of this Regulation and again at the earliest two years thereafter. The Commission should establish a process under which a product which is a candidate to be a critical product can be reviewed in a collaborative process by all relevant stakeholders, including manufacturers and users, to assess the security risk posed by potential cybersecurity issues with the product, whether and how much designating the product as critical would likely reduce that risk, and the costs associated with designating the product as critical, before adopting the relevant delegated acts.*

(27a) *The Commission should set up an expert group on cyber resilience (the ‘Expert Group’), with a wide and diverse membership. The Expert Group should support the Commission in order to ensure the proper implementation of this Regulation, for example by advising the Commission on possible amendments to the list of critical products set out in Annex III or by analysing in what way European and international standards can enable compliance with the essential requirements of this Regulation. The Commission should consult the Expert Group and carry out public consultations while preparing delegated and implementing acts pursuant to this Regulation, in order to ensure that all stakeholders can provide the necessary input.*

(28) This Regulation addresses cybersecurity risks in a targeted manner. Products with digital elements might, however, pose other safety risks, that are not *always* related to cybersecurity **but can be a consequence of a security breach**. 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 (EU) 2023/988. Therefore, in light of

the targeted nature of this Regulation, as a derogation from Article 2(1), third subparagraph, point (b), of Regulation **(EU) 2023/988**, Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation **(EU) 2023/988** 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 Regulation **(EU) 2023/988**.

(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation [\[22\]](#) [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 **(EU) 2023/1230 of the European Parliament and of the Council** [\[23\]](#) 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 **(EU) 2023/1230**, 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 ***do not fall*** 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 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 ***throughout the support period***, 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 ***make available their products without known exploitable vulnerabilities that might have an impact on the security of those products and to*** appropriately apply suitable harmonised standards, common specifications ***or international standards***.

(32a) ***Manufacturers should determine the support period during which they ensure that vulnerabilities are handled, duly taking into account various criteria, including the expected product lifetime, the nature of the product itself, the availability of the operating environment, the expectations of users, particularly consumers, and, where possible, the support period of other main components integrated into the product. Manufacturers should ensure that the support period adequately reflects the need to promote cybersecurity in the Union's market and is set with due consideration of the period during which a product with digital elements is expected to be available on the market. Market surveillance authorities should proactively ensure that manufacturers apply these criteria in an adequate manner. Market surveillance authorities and the Commission should collect and analyse data about the support periods set by manufacturers and the expected product lifetimes, in order to ensure that this Regulation meets its goal of promoting the cybersecurity of products with digital elements. Such***

analyses should, inter alia, inform the Commission's evaluation of this Regulation, once it applies.

(32b) Manufacturers should ensure, where technically feasible, that products with digital elements clearly differentiate between security and functionality updates. Security updates, designed to decrease the level of risk or to remedy potential vulnerabilities, should be installed automatically, in particular in the case of consumer products. Users should retain the possibility to de-activate this feature, with a clear and easy-to-use mechanism. Once the manufacturer no longer ensures that vulnerabilities of the product with digital elements are handled, it should inform users in a simple and clear manner, for example via the display of a user-friendly notification.

(32c) Where manufacturers set a support period of shorter than five years and no longer offer vulnerability handling for the product with digital elements, they should be able to make their source code available to undertakings that wish to provide security updates and other similar services. Such access should be made available only as part of a contractual arrangement that protects the ownership of the product with digital elements and prevents the dissemination of the source code to the public, except where such code has already been provided under a free and open-source licence.

(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 Directive (EU) 2022/2555⁵, 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 (EU) 2022/2555.

(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Directive (EU) 2022/2555 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 *disclose* fixed vulnerabilities to the

European vulnerability database established under Directive (EU) 2022/2555 and managed by ENISA¹. *ENISA should also publish notified vulnerabilities in the European vulnerability database and should have in place an appropriate procedure regarding the publication process in order to give manufacturers the time to develop the necessary security updates and users the time to implement them or take other corrective or mitigating measures. The European vulnerability database should assist manufacturers in detecting known exploitable vulnerabilities found in their products, in order to ensure that secure products are placed on the market.*

(34a) *The Union needs to maximise the benefits of its economic openness while minimising the risks from economic dependencies on high-risk vendors, through a common strategic framework for Union economic security^[24]. Dependencies on high-risk suppliers of critical products with digital elements pose a strategic risk that should be addressed at Union level, especially when the critical products with digital elements are intended for the use by essential entities of the type referred to in Directive (EU) 2022/2555. Such risks may be linked to the jurisdiction applicable to the manufacturer, the characteristics of its corporate ownership and the links of control to a third-country government where it is established, in particular whether a country engages in economic espionage and its legislation obliges arbitrary access to any kind of company operations or data, including commercially sensitive data, and can impose obligations for intelligence purposes without democratic checks and balances, oversight mechanism, due process or the right to appeal to an independent judiciary. Market surveillance authorities and the Commission should provide guidance and targeted recommendations to economic operators in order to ensure that appropriate corrective actions are put in place where there is sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of such non-technical risk factors.*

(35) Manufacturers should also report to ENISA any **significant** incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive **Directive (EU) 2022/2555** 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 (EU) 2022/2555** 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 **significant** 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 manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.

- (35a) Manufacturers and other entities and actors should also be able to report to ENISA, on a voluntary basis, about other cybersecurity incidents, cyber threats, near misses and any other vulnerability.***
- (35b) ENISA should establish a secure digital reporting mechanism that, in order to simplify reporting for manufacturers, should serve as a single entry point for reporting obligations established under this Regulation. Manufacturers of products with digital elements are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. The mechanism could, where possible, allow other Union law such as Regulation (EU) 2016/679, Directive (EU) 2022/2555 and Directive 2002/58/EC of the European Parliament and of the Council^[25] to be reported through the same mechanism. The mechanism may also be used for the voluntary notifications by manufacturers and other entities and actors. ENISA should ensure that they have procedures in place to handle classified information in a secure and confidential manner.***
- (35c) Entities and natural persons researching vulnerabilities may in some Member States be exposed to criminal and civil liability. The Commission should issue guidelines with regard to the non-prosecution of information security researchers and an exemption from civil liability for those activities.***
- (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 ***either directly to the manufacturer or indirectly, and where requested anonymously, via CSIRTs designated as a coordinator for the purposes of coordinated vulnerability disclosure in accordance with Article 12(1) of Directive (EU) 2022/2555.*** Manufacturers' 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').
- (36a) Member States and ENISA should make sure that vulnerabilities reported under this Regulation are not used by public bodies for intelligence, surveillance or offensive purposes.***
- (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 (**SBOMs**). A **SBOM** 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. ***Manufacturer should not, however, be obliged to make the software bill of materials public, as this may have unintended consequences on the cybersecurity of their products with digital elements.***

(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^[26]. 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. ***The standardisation process should ensure a balanced representation of interests and effective participation of civil society stakeholders, including consumer organisations. International standards should also be taken into account, in order to simplify the development of harmonised standards and the implementation of this Regulation, as well as to reduce non-tariff technical barriers to trade.***

(38a) Considering the broad scope of this Regulation, the timely development of harmonised standards poses a significant challenge. The Commission should ensure that harmonised standards will be in place by the date of application of this Regulation, in order to ensure the successful implementation 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 ***provide a common framework of trust for users to use*** products with digital elements covered by this Regulation. This Regulation should ***consequently*** 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 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 *delegated* acts, the European cybersecurity certification schemes that can be used to demonstrate conformity *for products with digital elements* with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, *there should be no* obligation for manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements *where a cybersecurity certificate has been issued under such European cybersecurity certification schemes, at a substantial or high level.*

(39a) In order to facilitate the compliance with this Regulation, the Commission should update the Union rolling work programme and request ENISA to prepare the missing candidate schemes in accordance with Article 48 of Regulation (EU) 2019/881.

(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 *delegated* acts, *after taking into account international standards. Such an option should be seen as an exceptional ‘fall back’ solution, where the standardisation process is blocked, where there are* undue delays in the establishment of appropriate harmonised standards, or *where the deliverables fail to comply with the initial* 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^[27]. 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^[28] 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 *risk-based and in most cases* 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 *those harmonised standards, common specifications or cybersecurity certification schemes have been in place for a minimum period of time enabling manufacturers to adopt them* and the manufacturer does not apply *them*, 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 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, ***in particular for microenterprises and small and medium-sized enterprises. In this regard, Member States, with the support of the Commission, should ensure that there is an adequate availability of skilled professionals in order to ensure that notified bodies can carry out their activities efficiently, thus minimising possible impediments, avoiding bottlenecks and facilitating economic operators' compliance with this Regulation.*** 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.

(53a) In order to increase efficiency and transparency, Member States should ensure, before the date of application of this Regulation, that there is a sufficient number of notified bodies in the Union to carry out conformity assessments. The Commission should monitor market developments and assist Member States in this endeavour, in order to avoid bottlenecks and hindrances to market entry.

(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^[29] 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 Directive (EU) 2022/2555 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) ***for the cyber resilience of products with digital elements*** 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 *provided* under which interested parties are informed of measures 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 **■ Directive (EU) 2022/2555** 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 **■ Directive (EU) 2022/2555**, 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 *that fall within* the scope of Directive **(EU) 2022/2555**, 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 *should* be organised to the market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives. ***The Commission should also coordinate market surveillance authorities in the regular inspections of products with digital elements that might present a security risk for the Union, including in light of the non-technical risk factor.***
- (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 *specifying 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*, the potential mandating of certification of certain highly critical products with digital elements based on criticality criteria 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. *Powers to adopt delegated acts should also be delegated to the Commission to specify the format and elements of the software bill of materials, specify further the format and procedure of the notifications on actively exploited vulnerabilities and significant incidents submitted to ENISA by the manufacturers. Where necessary, the Commission should be empowered to adopt delegated acts to adopt common specifications in respect of the essential requirements set out in Annex I.* 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^[30]. 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. *For the purpose of developing delegated acts pursuant to this Regulation, the Commission should consult the cyber resilience Expert Group. The Commission should also conduct regular structural dialogue with economic operators and carry out public consultations, inter alia for the purposes of evaluating the scope of this Regulation and whether certain categories of products should be included or excluded.*

- (63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to: **■** lay down technical specifications for *labelling schemes, including harmonised labels*, 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 powers should be exercised in accordance with

Regulation (EU) No 182/2011 of the European Parliament and of the Council^[31].

- (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 *the manufacturer is a microenterprise, a small or medium-sized enterprise or a start-up and* 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.
- (66a) *The revenues generated from the payments of penalties should be used to strengthen the level of cybersecurity within the Union, including by developing capacity and skills related to cybersecurity, improving economic operators' cyber resilience, in particular of microenterprises and of small and medium-sized enterprises and more in general fostering public awareness of cyber security issues.*

- (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 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 *the Expert Group and other* 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 [36 months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [18 months] from the entry into force of this Regulation.
- (69a) This Regulation will generate additional costs for microenterprises and small and medium-sized enterprises, including start-ups. In order to support these enterprises, the Commission should establish financial and technical support that enable these enterprises to contribute to the growth of the European economy and the European cybersecurity landscape, including by streamlining the financial support from the Digital Europe Programme and other relevant Union programmes as well as supporting companies and public sector organisations through European Digital Innovation Hubs. Furthermore, Member States should consider all possible complementary actions aiming to providing guidance and support for microenterprises and for small and medium-sized enterprises, including via the establishment of regulatory sandboxes, cybersecurity hubs and start-up accelerators.***

(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^[32] and delivered its opinion on **9 November 2022**^[33].

(71a) The Commission should amend the legislative financial statement accompanying this Regulation by providing ENISA with nine additional full-time equivalent and corresponding additional appropriations in order to fulfil its additional tasks provided for in this Regulation,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This Regulation lays down:

- (a) rules for the ***making available*** 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 ***monitoring***, surveillance and enforcement of the above-mentioned rules and requirements.

Article 2

Scope

1. This Regulation applies to products with digital elements ***made available on the market that can have*** a direct or indirect ■ data connection to a device or network.
2. This Regulation does not apply to products with digital elements to which the following Union ***legislative*** 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.
- 3a. This Regulation applies to free and open-source software only where such software is made available on the market in the course of a commercial activity.***
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.

4a. This Regulation does not apply to spare parts that are exclusively manufactured to replace identical parts and that are supplied by the manufacturer of the original products with digital elements.

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 *or on behalf 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);
- (4a) ‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;**
- (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, ***monetisation*** 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;
- (21a) ‘microenterprises’, ‘small enterprises’ and ‘medium sized enterprises’ means microenterprises, small enterprises and medium-sized enterprises as defined in Commission Recommendation 2003/361/EC^[34];***
- (21b) ‘consumer’ means any natural person who, under the circumstances of this Regulation, is acting for purposes which are outside their trade, business, craft or profession;***
- (21c) ‘support period’ means the period during which the manufacturer ensures that vulnerabilities of the product with digital elements are handled effectively and in accordance with the essential requirements set out in Annex I, Section 2;***
- (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, ***excluding necessary security updates that aim to mitigate vulnerabilities***;
- (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;

- (34a) *‘international standard’ means an international standard as defined in Article 2, point (1)(a) of Regulation (EU) No 1025/2012;*
- (35) *‘risk’ means risk as defined in Article 6, point (9) of Directive (EU) 2022/2555;*
- (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’ or ‘SBOM’ 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 6, point (15) of Directive (EU) 2022/2555;*
- (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;*
- (39a) *‘incident’ means an incident as defined in Article 6, point (6) of Directive (EU) 2022/2555;*
- (39b) *‘near miss’ means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;*
- (39c) *‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;*(40) *‘personal data’ means data as defined in Article 4, point (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. ■ Member States shall not prevent the presentation and use of a **prototype** product with digital elements which does not comply with this Regulation, ***provided that the availability of such a product is limited in time and geographical area and is supplied exclusively for testing and, where possible, a visible sign indicating its non-compliance.***
3. Member States shall not prevent the making available ***free of charge*** 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.

- 3a. Member States, if applicable with the support of ENISA, may establish controlled testing environments for innovative products to facilitate their development. In that context, particular support shall be provided for microenterprises, small and medium-sized enterprises, including start-ups.**

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, ***provided with the necessary security and functionality updates***, 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.

The integration of a product of higher class of criticality does not change the level of criticality for the product into which it is integrated.

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. ***The first such delegated act may be adopted no earlier than two years after the date of entry into force of this Regulation. Any subsequent delegated act may be adopted at the earliest two years thereafter.*** 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 **Article 3 of Directive (EU) 2022/2555**;
- (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 ... [] 6 months after* 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).

Where a new category of critical products with digital elements is added to class I or II as set out in Annex III by means of a delegated act pursuant to paragraph 2 of this Article, it shall be subject to the relevant conformity assessment procedures referred to in Article 24(2) and (3) of this Regulation within 12 months of the date of adoption of the delegated act concerned.

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 ***at assurance level 'high'*** pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. ***The obligation to obtain a European cybersecurity certificate shall apply within 12 months of the adoption of the relevant delegated act.*** 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 Article 3 of Directive (EU) 2022/2555* 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.

5a. The Commission is empowered to adopt the delegated acts referred to in paragraph 5 of this Article no earlier than 12 months after the adoption of the relevant European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881.

Article 6a

Expert Group on cyber resilience

1. By ... [6 months after the date of entry into force of this Regulation], the Commission shall establish an expert group on cyber resilience (the 'Expert Group'). The Expert Group shall be appointed for a renewable three-year term by the Commission. The composition of the Expert Group shall aim to be gender and geographically balanced and shall include the following:

(a) representatives of each of the following:

- (i) the European Union Agency for Cybersecurity;*
- (ia) the European Cybersecurity Competence Centre;*
- (ii) the European Data Protection Board;*
- (iii) European standardisation bodies.*

Where needed, representatives of other Union Agencies may be invited.

- (b) experts representing relevant economic operators, ensuring the adequate representation of microenterprises and small and medium-sized enterprises;*
- (c) experts representing civil society, including consumer organisations and the free and open-source community;*
- (d) experts appointed in a personal capacity, who have proven knowledge and experience in the areas covered by this Regulation;*
- (e) experts representing academia, including universities, research institutes and other scientific organisations, including persons with global expertise.*

2. The Expert Group shall advise the Commission with regard to the following:

- (a) the list of critical products with digital elements set out in Annex III, as well as on the possible need to update that list;*
- (b) the implementation of European cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 and on the possibility to make them mandatory for highly critical products with digital elements;*
- (c) non-binding evaluations of products with digital elements upon request by a market surveillance authority that is conducting an investigation under Article 43;*
- (d) the application of relevant concepts of the new legislative framework to software, in particular free and open-source software;*
- (e) the elements of the Regulation to be addressed by the guidelines referred to in Article 17a;*
- (f) the availability and the quality of European and international standards, and the possibility to supplement or replace them with common technical specifications;*
- (g) the availability of skilled professionals in the field of cybersecurity across the Union, including of adequate personnel to perform third-party conformity assessments pursuant to this Regulation;*
- (h) the possible need to amend this Regulation.*

The Expert Group shall also map trends at Union and Member State level regarding existing and patched vulnerabilities.

3. The Expert Group shall take into account the views of a wide range of stakeholders and perform their tasks with highest level of professionalism, independence, impartiality and objectivity.

3a. The Commission shall consult the Expert Group when preparing delegated or implementing acts based upon this Regulation.

3b. The Expert Group may provide market surveillance authorities with non-binding evaluations of products with digital elements to facilitate investigations under Article 43.

4. The Expert Group shall be chaired by the Commission and shall be constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. In that context, the Commission may invite experts with specific expertise on an ad hoc basis.

5. The Expert Group shall carry out its tasks in accordance with the principle of transparency. The Commission shall publish the composition of the Expert Group, the declaration of interests of its members, a summary of the meetings of the Expert Group and other relevant documents on the Commission website.

Article 6b

Enhancing skills in a cyber resilient digital environment

For the purpose of this Regulation and in order to respond to the demand of professionals capable of ensuring the cybersecurity of products with digital elements, the Commission and Member States, in cooperation with ENISA, shall ensure the implementation of:

- (a) education and training programmes in the cyber security field and their associated career pathways, contributing to making the cyber security workforce more resilient and inclusive, also in terms of gender and aligned with the needs of undertakings concerned, in particular where such undertakings are microenterprises, small or medium-sized enterprises, including start-ups, or public administration;*
- (b) initiatives to increase the collaboration between the private sector, economic operators, including via re-skilling or up-skilling for manufacturers' employees, consumers, education and training providers as well as Member States, expanding the options for young people to access jobs in this sector;*
- (c) strategies aiming to enhance workforce mobility, developing cyber security skills and creating organisational and technological tools to maximise existent cyber security talent.*

Article 7

General product safety

By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation **(EU) 2023/988** 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 Regulation **(EU) 2023/988**, Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation **(EU) 2023/988** 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, **relevant** 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 **that fall** 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.
- 3a. Manufacturers of products with digital elements classified as high-risk AI systems in accordance with paragraph 1 of this Article may participate in the AI regulatory sandboxes referred to in Article 53 of Regulation [the AI Regulation].**

Article 9

Machinery products

Machinery products **that fall within** the scope of Regulation (EU) 2023/1230 which are **products with digital elements or partly completed** 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 (EU) 2023/1230, 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.

Article 9a

Public procurement of products with digital elements

1. *Without prejudice to Directives 2014/24/EU[35] and 2014/25/EU[36] of the European Parliament and of the Council, Member States shall ensure, when procuring products with digital elements, a high level of cybersecurity and an appropriate support period.*
2. *Member States shall ensure that manufacturers remedy vulnerabilities in publicly procured products with digital elements, including by making security updates available promptly.*

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.
 - 2a. *On the basis of the cybersecurity risk assessment, manufacturers shall determine how the essential requirements set out in Section 1 of Annex I are applicable to their product with digital elements. They shall include the risk assessment in the technical documentation as set out in Article 23.3.* 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. *It falls upon the manufacturer to ensure that such components do not compromise the security of the product with digital elements, including when integrating*

components of free and open-source software that have not been made available on the market in the course of a commercial activity.

Manufacturers shall, upon identifying a vulnerability in a component, including in a free and open-source component, which is integrated in the product with digital elements, address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Annex I, Section 2, and share the corrective measures taken with the person or entity maintaining the component.

4a. The manufacturer of components shall provide to the manufacturer of the final product with digital elements the information and documentation necessary to comply with the requirements of this Regulation, when supplying them with such components. This information shall be provided free of charge.

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, *manufacturers shall determine the support period during which* vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I. *In doing so, the manufacturer shall ensure that the support period is proportionate to the expected product lifetime as well as in line with the nature of the product and users' expectations, the availability of the operating environment and, where applicable, the support period of the main components integrated into the product with digital elements. To that end manufacturers shall make available upon request of market surveillance authorities information on the expected product lifetime they considered in order to determine the duration of the support period for the product made available on the market. Market surveillance authorities shall monitor products with digital elements and ensure actively that manufacturers have applied these criteria in an adequate manner, including an assessment of the information received from the manufacturers on the expected product lifetime, when determining the support period.*

Where applicable, the support period shall be clearly stated on the product, its packaging or be included in contractual agreements. In any case, end users shall also be informed before purchase of the duration of the support period.

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.

Where applicable, for consumer products with digital elements, those procedures shall include automatic security updates by default. Users should retain the possibility of de-activating those automatic security updates.

Manufacturers shall actively inform users when their product with digital elements has reached the end of its support period.

6a Where the support period is shorter than five years and the handling of vulnerabilities has ended, manufacturers may provide access to the source code of such a product with digital elements to other undertakings which commit to extending the provision of vulnerability handling services, in particular security updates. Access to such source codes shall be provided only where provided for in a contractual arrangement. Those arrangements shall protect the ownership of the product with digital elements and shall prevent the dissemination of the source code to the public, except where such code has already been provided under a free and open-source licence.

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 at the disposal of the market surveillance authorities for *at least ten years or the support period, whichever is longer*, after the product with digital elements has been placed on the market.

Market surveillance authorities shall ensure the confidentiality and appropriate protection of the information in the technical documentation provided by manufacturers in accordance with Article 52.

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 *horizontal or sector specific* 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.

Where such information and instructions are provided in electronic form, manufacturers shall:

(a) present them in a user-friendly format that makes it possible for the user to consult them online, download them, save them on an electronic device and print them;

(b) ensure that they are accessible online during at least the support period of the product 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 *at least the support period* **■**, 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, *after consulting the Expert Group and taking account of international standards, is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I.* ■

Article 11

Reporting obligations of manufacturers

1. The manufacturer shall ■ notify to ENISA any actively exploited vulnerability contained in the product with digital elements *in accordance with paragraph 1a of this Article.* ■ 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 12 of Directive (EU) 2022/2555 of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability. *Where a notified vulnerability has no corrective or mitigating measures available, ENISA shall ensure that information about the notified vulnerability is shared in line with strict security protocols and on a need-to-know-basis.*

1a. Notifications as referred to in paragraph 1 shall be subject to the following procedure:

- (a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the existence of an actively exploited vulnerability, including whether any known corrective or recommended risk mitigating measure is available;*
- (b) a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which, where applicable, updates the general information referred to in point (a), including any corrective or mitigating measures taken and indicates an assessment of extent of the vulnerability, including its severity and impact;*
- (c) a final report, within one month after the submission of the vulnerability notification under point (b) or when a corrective or mitigating measure is available, including at least the following:*
 - (i) a description of the vulnerability, including its severity and impact;*
 - (ii) where available, information concerning any actor that has exploited or that is exploiting the vulnerability;*

(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.

1b. After a security update is made available or another form of corrective or mitigating measures is put in place, ENISA shall add the notified vulnerability pursuant to paragraph 1 of this Article to the European vulnerability database referred to in Article 12 of Directive (EU) 2022/2555.

2. The manufacturer shall **■** notify to ENISA any **significant** incident having impact on the security of the product with digital elements **in accordance with paragraph 2b of this Article**. 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 8 of Directive (EU) 2022/2555 of the Member States concerned and inform the market surveillance authority about the notified incidents. The **mere act of notification shall not subject the notifying entity to increased liability**.

2a. An incident shall be considered to be significant as referred to in paragraph 2, where:

(a) it has caused or is capable of causing severe operational disruption of the production or the services for the manufacturer concerned, which would impact the security of a product; or

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

2b. Notifications as referred to in paragraph 2 shall be subject to the following procedure:

(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the significant incident, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the significant incident, which, where applicable, shall update the information referred to in point (a) and indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) a final report, within one month after the submission of the incident notification under point (b), including at least the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

In the event of an ongoing incident at the time of the submission of the final report referred to in point (d) of this paragraph, Member States shall ensure that the manufacturer concerned provides a progress report at that time and a final report within one month of their handling of the incident.

2c. Manufacturers that have notified significant incidents according to this Regulation and that are also identified as essential entities or important entities under the Directive (EU) 2022/2555 shall be deemed compliant with the requirements under Article 23 of Directive (EU) 2022/2555. ENISA shall forward the notifications received pursuant to this Regulation to the responsible CSIRT according to Directive (EU) 2022/2555. An entity may only be fined once for non-compliance with overlapping requirements.

2d. Where necessary, ENISA or the relevant CSIRT may request manufacturers to provide an intermediate report on relevant status updates about the actively exploited vulnerability or significant incident.

2e. Manufacturers that qualify as microenterprises or as small or medium-sized enterprises shall be exempt from paragraph 1a, point (a) and paragraph 2b, point (a).

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by Article 16 of Directive (EU) 2022/2555 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 **impacted** users of the product with digital elements , **and where appropriate all users**, about the **significant** incident and, where necessary, about **risk mitigation and any** corrective measures that the user can deploy to mitigate the impact of the **significant** incident.

4a. ENISA shall ensure that notifications pursuant to paragraphs 1 and 2 are submitted via channels of communication and stored on servers that ensure the highest possible levels of cybersecurity and protection from malicious actors.

4b Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, ENISA and, where appropriate, the CSIRTs or the competent authorities of the relevant Member States,

may, after consulting the manufacturer concerned, inform the public about the significant incident or require the manufacturer to do so.

5. The Commission *shall adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying* further the **■** format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those *delegated* acts shall be adopted *by ... [12 months after the date of entry into force of this Regulation]*.
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 *14* of Directive (EU) 2022/2555. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying. *ENISA shall include relevant information from its technical reports in its report on the state of cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555.*
- 6a. *ENISA shall establish a secure digital reporting mechanism, after having consulted the Expert Group, in order to simplify reporting obligations of manufacturers. This mechanism shall serve as a single entry point for reporting obligations established under this Regulation and, where possible, other Union law.*

■ Article 11a *Voluntary notification*

1. *In addition to the notification obligations set out in Article 11, notifications may be submitted to ENISA on a voluntary basis by the following:*
 - (a) *manufacturers, with regard to incidents, cyber threats and near misses;*
 - (b) *entities other than those referred to in point (a), regardless of whether they fall within the scope of this Regulation, with regard to significant and non-significant incidents, cyber threats and near misses;*
 - (c) *any actor with regard to vulnerabilities which may be included in the European vulnerability database referred to in Article 12 of Regulation 2022/2555.*
2. *ENISA shall process the notifications referred to in paragraph 1, point (a) of this Article in accordance with the procedure laid down in Article 11. ENISA may prioritise the processing of mandatory notifications over voluntary notifications.*
3. *In order to simplify the voluntary notifications, it shall be possible to notify these through the secure digital reporting mechanism referred to in Article 11(6a).*

4. *Where appropriate, ENISA shall ensure the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.*

Article 11b

Point of single contact for users

1. *In order to facilitate reporting on the security of products, manufacturers shall designate a point of single contact to enable users to communicate directly and rapidly with them, where applicable by electronic means and in a user-friendly manner, including by allowing users of the product to choose the means of communication set out in point 1 of Annex II, which shall not solely rely on automated tools.*
2. *In addition to the obligations provided under Directive 2000/31/EC of the European Parliament and of the Council [\[37\]](#), manufacturers shall make public the information necessary for the end users in order to easily identify and communicate with their points of single contact. That information shall be easily accessible and shall be kept up to date.*

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. ***It shall provide a copy of the mandate to the market surveillance authorities upon request.*** 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;
 - (aa) ***where the authorised representative has a reason to believe that a product with digital elements in question presents a cybersecurity risk, inform the manufacturer;***
 - (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 **effectively** 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, **the EU declaration of conformity is available** and **the product** is accompanied by the information and instructions for use as set out in Annex II;

(ca) all the documents proving the fulfilment of the requirements set out in this Article have been received from the manufacturer.
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.

On the basis of targeted recommendations received by market surveillance authorities or by the Commission in accordance with Articles 43 and 45, an importer shall apply such recommendations, including withdrawing or recalling the product. Additionally, where an importer considers or has reasons to believe that a product with digital elements may present a cybersecurity risk in light of non-technical risk factors, it shall withdraw or recall that product. Importers shall inform the market surveillance authorities and the Commission to that effect.

4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and the email address, **and where available, the website**, at which they can be contacted on the product with digital elements or  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 ***request the manufacturer to*** 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.
- 6a. Upon ***becoming aware of*** 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), **and have communicated all relevant documents to the distributor;**
3. Where a distributor considers or has reason to believe, ***on the basis of information in its possession***, 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, ***on the basis of information in their possession***, 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 ***request the manufacturer to take*** 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.
 - 4a. Upon ***becoming aware of*** 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. ***On the basis of information in its possession***, 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 ***and makes it available on the market***, 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, 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.

Article 17a

Guidelines

- 1. In order to create clarity, certainty for, and consistency among the practices of economic operators, the Commission shall prepare and issue guidelines for economic operators, explaining how to apply this Regulation, with a particular focus on how to facilitate compliance by microenterprises, small enterprises and medium-sized enterprises.*
- 2. The guidelines shall be published by ... [12 months after the date of entry into force of this Regulation] and shall be updated as necessary, in particular in light of potential amendments to the list of critical products set out in Annex III. They shall contain at least the following elements:*
 - (a) a detailed explanation of the scope of this Regulation, with a particular focus on remote data processing solutions and free and open-source software;*
 - (b) detailed criteria used to determine how critical products with digital elements are placed in classes I or II as set out in Annex III;*
 - (c) the interplay between this Regulation and other Union law, particularly concerning presumptions of conformity and conformity assessments;*
 - (d) guidance for manufacturers on how to perform the cybersecurity risk assessment referred to in Article 10(2) and on the applicability of the essential requirements including where available best practices ;*
 - (e) guidance for manufacturers on how to determine appropriately the support period for different product categories in accordance with Article 10(6);*
 - (f) an explanation of how to handle reporting requirements pursuant to this Regulation or other Union law;*
 - (g) a list of the delegated and implementing acts published by the Commission pursuant to this Regulation;*
 - (h) guidance for Member States on the non-prosecution of information security researchers;*
 - (i) guidance on what constitutes substantial modifications.*
- 3. When preparing the guidelines pursuant to this Article, the Commission shall consult the Expert Group.*

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.

The Commission shall in accordance with Article 10(1) of Regulation (EU) 1025/2012 request one or more European standardisation organisations to draft harmonised standards for the essential requirements set out in Annex I to this Regulation. When preparing the standardisation request for this Regulation, the Commission shall strive to take into account existing or imminent international standards for cybersecurity in order to simplify the development of harmonised standards.

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 ***to adopt***, by means of ***delegated*** acts ***in accordance with Article 50, to supplement this Regulation by*** specifying the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity ***of products with digital elements*** with the essential requirements or parts thereof as set out in Annex I. Furthermore, ***the issuance of*** a cybersecurity certificate issued under such schemes, ***at assurance level ‘substantial’ or ‘high’***, 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). ■

Article 19

Common specifications

1. ■ The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by establishing common specifications that cover technical requirements providing a means to comply with the requirements set out in Annex I for products that fall within the scope of this Regulation where the following conditions have been fulfilled:
 - (a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the essential requirements set out in Annex I and the request has not been accepted or the European standardisation deliverables addressing that request is not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012 or European standardisation deliverables do not comply with the request; and
 - (b) no reference to harmonised standards covering the relevant essential requirements set out in Annex I to this Regulation is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.
2. Before preparing the delegated act, the Commission shall inform the Expert Group that it considers that the conditions in paragraph 1 are fulfilled. In preparing the delegated acts, the Commission shall take into account the opinions of the Expert Group.
3. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the publication of its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference to a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the relevant delegated acts referred to in paragraph 1, or the parts thereof which cover the same essential requirements set out in Annex I to this Regulation.

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 ■ updated *as appropriate*. 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. ***In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.***
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. *After consulting the Expert Group, the dedicated administrative cooperation group (ADCO) and, where necessary, other relevant stakeholders*, the Commission may, by means of implementing acts, lay down technical specifications for **labelling schemes, including harmonised labels**, pictograms or any other marks related to the security of the products with digital elements, **their support period** and mechanisms to promote their use **among businesses and consumers and to increase public awareness about the security of products with digital elements**. 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 **at least the support period**.
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. ***The Commission shall ensure that the administrative burden on microenterprises and small and medium-sized enterprises is proportionate.***

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;

(ca) a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881 in accordance with Article 18(4).
 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 ***at assurance level 'substantial' or 'high'*** 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.
- 2a. Harmonised standards, common specifications or European cybersecurity certification schemes shall be in place for six months before the conformity assessment procedure referred to in paragraph 2 of this Article applies. In***

the six months prior to the application of paragraph 2 of this Article, or where, harmonised standards, common specifications or European cybersecurity certification schemes do not exist, manufacturers shall demonstrate the conformity of the critical product with digital elements of class I as set out in Annex III by means of the procedure referred to in paragraph 1 of this Article.

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) a European cybersecurity certificate, under a European cybersecurity certification scheme at assurance level 'substantial' or 'high' pursuant to Regulation (EU) 2019/881;

(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.

3a. The Commission shall request ENISA to prepare the missing candidate schemes in accordance with Article 48 of Regulation (EU) 2019/881.

4. Manufacturers of products with digital elements that are classified as EHR systems under ■ 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 *microenterprises and* small and medium-sized enterprises ■ when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs. *The Commission shall ensure appropriate financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and on small and medium-sized enterprises.*

Article 24a

Mutual recognition agreements

In order to promote international trade, the Commission shall endeavour to conclude Mutual Recognition Agreements (MRAs) with third countries. The Union shall establish MRAs only with third countries that are on a comparable level of technical development and have a compatible approach concerning conformity

assessment. The MRAs shall ensure the same level of protection as that provided for by this Regulation.

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.

6a. A notifying authority shall minimise administrative burden and fees imposed, in particular, on microenterprises and small and medium-sized enterprises.

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.

1a. Member States shall, by ... [24 months after the date of entry into force of this Regulation], ensure that there is a sufficient number of notified bodies in the Union to carry out conformity assessments, in order to avoid bottlenecks and hindrances to market entry.

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 *set out in Annex I*, 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.

7a. Member States and the Commission shall put in place appropriate measures to ensure sufficient availability of skilled professionals, in order to minimise bottlenecks in the activities of conformity assessment bodies and facilitate the compliance of economic operators with this Regulation.

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 *in accordance with Article 52*. 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 accordance with Article 37(2)*, in particular taking into account the interests of *microenterprises and small and medium-sized enterprises* 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, ***with consideration for microenterprises and small and medium-sized enterprises***. 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 ***and the risk exposure*** of the product ***type and*** 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, ***taking also in account the need to reduce the administrative burden and fees***, 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 ***that fall*** 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, ***competent authorities and CSIRTs designated pursuant to Directive (EU) 2022/2555*** and exchange information on a regular basis. **■**
- 3a. ***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. The market surveillance authorities may request ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 43, market surveillance authorities may request ENISA to provide non-binding evaluations of compliance of products with digital elements.***
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, ***with appropriate cybersecurity skills, in order*** to fulfil their tasks under this Regulation.

7. The Commission shall facilitate the ***regular and structured*** 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 ***as well as on non-technical risk factors***, with the support of ***CSIRTs, ENISA and*** the Commission.

8a. Market surveillance authorities shall be equipped to receive complaints by consumers in accordance with Article 11 of Regulation 2019/1020, including by establishing clear and accessible mechanisms to facilitate reporting of vulnerabilities, incidents and cyber threats.

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.

Market surveillance authorities shall provide the Commission with data about the average support period set by the manufacturers, as well as when available the average expected product lifetime, and disaggregated per category of product with digital elements. The Commission shall analyse this information and publish it in a publicly accessible and user-friendly database.

9a. The Commission shall evaluate the reported data including pursuant to paragraph 9 of this Article for the purpose of the reports referred to in Article 56. Where the reported data suggests an increased level of non-compliance in specific categories of products, the Commission, after consulting the Expert Group and ADCO, may recommend that surveillance authorities focus closely on the product categories concerned.

10. For products with digital elements ***that fall within*** 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. An **ADCO for cyber resilience of products with digital elements** 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. ***In particular, this ADCO shall exchange best practices and, where relevant, cooperate with the Expert Group and ENISA as well as the Cooperation Group and the CSIRTs Network referred to under Directive (EU) 2022/2555.***

11a. Market surveillance authorities shall facilitate the involvement of stakeholders, including scientific, research and consumer organisations, in their activities.

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 ***without undue delay, and where appropriate in cooperation with CSIRT***, 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 ***economic*** 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.

1a. Where the market surveillance authority of a Member State has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk or threats to national security in light of non-technical risk factors, it shall issue targeted recommendations to economic operators aimed at ensuring that appropriate corrective actions are put in place.

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 reason 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 ***shall*** request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.
 - 1a. ***Where the Commission has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of non-technical risk factors, it shall inform the relevant market surveillance authorities and issue targeted recommendations to economic operators aimed at ensuring that appropriate corrective actions are put in place.***
2. In **■** 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 ***shall*** 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 **Article 3 of Directive (EU) 2022/2555** or to other aspects of public interest protection, it shall require the relevant *economic* 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 *economic* 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 ■ 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 ***shall*** establish **■** a corrective or restrictive measure ***at Union level*** if necessary. 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 **shall** 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 **shall** 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 **that fall within** 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 **shall regularly** 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. ***They shall include inspections of products acquired under a cover identity and shall aim to verify the compliance of those products with 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 **shall** make the aggregated results publicly available.
3. ENISA **shall** 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 **shall** 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 *in* Articles 41 to 47 and any other powers conferred upon them by national law.
5. Market surveillance authorities *shall* 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 10(15), Article 11(5), Article 18(4), Article 19(1)**, 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 10(15), Article 11(5), Article 18(4), Article 19(1)**, 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 10(15), Article 11(5), Article 18(4), Article 19(1)**, Article 20(5) *or* 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[\[38\]](#);
 - (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 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. ***Member States shall ensure that those rules take into account the financial capabilities of microenterprises and small and medium-sized enterprises.***
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. ***The Commission shall ensure that those rules and measures are applied in a uniform and consistent manner across the Union.***
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;
 - (aa) whether the infringement is unintentional;***
 - (b) whether administrative fines have been already applied by ***the same or*** other market surveillance authorities to the same operator for a similar infringement;

- (c) the size, *in particular with regard to microenterprises, small and medium sized-enterprises, including start-ups*, 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.

Article 53a

Allocation of the revenue from penalties

Member States shall allocate the revenues from the penalties referred to in Article 53(1) to projects raising the level of cybersecurity within the Union. Those projects shall aim at least to one of the following:

- (a) increase the number of skilled professionals in the field of cybersecurity, notably women;*
- (b) increase capacity-building for microenterprises and small and medium-sized enterprises in order to facilitate their compliance with this Regulation;*
- (c) improve public awareness of cyber threats, with particular regard to their prevention and management;*
- (d) develop tools to increase the resilience of Union undertakings to cyber-enabled intellectual property theft.*

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 54a

Amendment to Directive (EU) 2020/1828

In Annex I to Directive (EU) 2020/1828 of the European Parliament and of the Council^[39] the following point is added:

‘67. [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 *that fall* 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].

3a. Until the date of application of this Regulation, manufacturers may comply with the requirements of this Regulation on a voluntary basis. Where manufacturers comply with this Regulation with regard to their products with digital elements, they shall be considered also to comply with Delegated Regulation (EU) 2022/30.

The Commission shall repeal Delegated Regulation (EU) 2022/30 on the same date of application of this Regulation.

Article 56

Evaluation and review

1. 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.
2. ***Every year when presenting the Draft Budget for the following year, the Commission shall submit a detailed assessment of ENISA's tasks under***

this Regulation as set out in Annex VIa and other relevant Union law and shall detail the financial and human resources needed to fulfil those tasks.

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 [36 months after the date of entry into force of this Regulation]. However Article 11 shall apply from [18 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 ...■ ,

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

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;

■

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

(-a) be made available without known exploitable vulnerabilities;

- (a) be *made available* with a secure by default configuration, *unless otherwise agreed between the parties in a business-to-business context*, including the possibility to reset the product to its original state *while retaining all installed security updates*;

(aa) where technically feasible, be made available on the market with functional separation of security updates from functionality update;

- (ab) ensure automatic security updates with a clear and easy-to-use opt-out mechanism and the notification of available updates to users;**
- (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, **and by using other technical means;**
- (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 **or possible unauthorised access;**
- (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 **and basic** functions, **also after an incident**, including **with backup management**, and the resilience and mitigation **measures against** 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 **capabilities for** relevant internal activity, including the access to or modification of data, services or functions, **with an opt-out mechanism for the user;**



(ka) enable users to securely withdraw and remove their data on a permanent basis.

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

- (1) 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;
- (2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates ***installed automatically where applicable in accordance with Section I;***
- (3) apply effective and regular tests and reviews of the security of the product with digital elements;
- (4) once a security update has been made available, ***share and*** publicly disclose information about fixed vulnerabilities ***in a controlled way***, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and ***clear and accessible*** information helping users to remediate the vulnerabilities;
- (5) put in place and enforce a policy on coordinated vulnerability disclosure;
- (6) 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;
- (7) provide for mechanisms to securely distribute ***security*** updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;
- (8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and ***unless otherwise agreed between the parties in a business-to-business context***, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken;
- (8a) ***where possible and applicable, notify the user of the end of the support period.***

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 *and where available the website* at which the manufacturer can be contacted, on the product or on its packaging or in a document accompanying the product;
2. the point of *single* contact where information about cybersecurity vulnerabilities of the product can be reported and received *and the manufacturer's policy on coordinated vulnerabilities and where it can be found*;
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 *by the competent authorities in accordance with non-disclosure conditions set out in Article 52*;
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 *the support period during which* users can expect *vulnerabilities to be handled and* 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

1. Identity management systems software and privileged access management software;
2. Standalone and embedded browsers;
3. Password managers;

3a. Biometric readers;

4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Network configuration management tools;
8. Network traffic monitoring systems;
9. Management of network resources;
10. Security information and event management (SIEM) systems;
11. Update/patch management, including boot managers;
12. Application configuration management systems;
13. Remote access ■ software;
14. Mobile device management software;
15. Physical **and virtual** network interfaces;
16. Operating systems not covered by class II;
17. Firewalls, intrusion detection and/or prevention systems not covered by class II;
19. **General purpose microprocessors and** microprocessors not covered by class II;
20. Microcontrollers;
21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in **Article 3 of Directive(EU) 2022/2555**;
22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC), **industrial robots and their control systems** and supervisory control and data acquisition systems (SCADA);
23. Industrial Internet of Things not covered by class II;
- 23a. Home automation systems, including smart home servers and virtual assistants;**

23b. Security devices, including smart door locks, cameras and alarm systems;

23c. Smart toys;

23d. Personal health appliances and wearables.

Class II

1. Operating systems for servers, desktops, and mobile devices;
2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
3. Public key infrastructure and digital certificate issuers;
4. Firewalls, intrusion detection and/or prevention systems intended for industrial use;
5. Secure elements;
6. Microprocessors intended for integration in programmable logic controllers and secure elements;
7. Routers, modems intended for the connection to the internet, and switches ;
8. Secure elements;
9. Hardware Security Modules (HSMs);
10. Secure cryptoprocessors;
11. Smartcards, smartcard readers and tokens;
12. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in **Article 3 of Directive (EU) 2022/2555**, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in **Article 3 of Directive (EU) 2022/2555**;
14. Secure elements;
15. 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:

1. Name and type and any additional information enabling the unique identification of the product with digital elements;
2. Name and address of the manufacturer or his authorised representative;
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;
4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);
5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;
6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;
7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;
8. 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:

1. a general description of the product with digital elements, including:
 - (a) its intended purpose;
 - (b) versions of software affecting compliance with essential requirements;
 - (c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;
 - (d) user information and instructions as set out in Annex II;
2. a description of the design, development and production of the product and vulnerability handling processes, including:

- (a) 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;
 - (b) 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;
 - (c) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.
- 3. 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, ***including how the essential requirements set out in Annex I, Section 1, are applicable***;
- 4. 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;
- 5. 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;
- 6. a copy of the EU declaration of conformity;
- 7. 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)

1. 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.

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

3. 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.

4. Conformity marking and declaration of conformity

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

4.2. 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 *or the support period, whichever is longer*. 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.

5. 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)

1. 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.

2. 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).
3. 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.

4. The notified body shall:

- 4.1. 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;
- 4.2. 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;

- 4.3. 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;
- 4.4. 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;
- 4.5. agree with the manufacturer on a location where the examinations and tests will be carried out.
5. 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.
6. 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.

7. 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.

8. 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.

9. 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 *or for the support period*.
10. 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)

1. 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.

2. Production

2.1. 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.

3. Conformity marking and declaration of conformity

3.1. 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.

3.2. 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 *or for the support period*. 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.

4. 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)

1. 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.

2. 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.

3. Quality system

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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.

4. Surveillance under the responsibility of the notified body

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

4.2. 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.

4.3. 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.

5. Conformity marking and declaration of conformity

5.1. 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.

5.2. 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 *or for the support period*. 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.

6. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market *or for the support period or the period during which vulnerabilities are handled*, 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.

7. 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.

8. 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.

ANNEX VIa

CAPACITY NEEDS OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

In order to fulfil its obligations under this Regulation and in order not to compromise existing obligations of the Agency under other Union law, the adequate staffing and financing of ENISA shall be ensured. Therefore additional tasks for ENISA under this Regulation shall be accompanied by additional human and financial resources. Nine additional full-time equivalent and corresponding additional appropriations will be needed to cover the additional tasks under this Regulation.

EXPLANATORY STATEMENT

The Rapporteur strongly welcomes the Commission proposal to address cybersecurity deficiencies in hardware and software products. In 2021, the global cost of cybercrime has reached a staggering EUR 5.5 trillion. This phenomenon, coupled with the upward trend of digitalisation, calls on legislators to ensure that appropriate cybersecurity measures are in place to safeguard the interests of both consumers and industry.

On this note, the Rapporteur is pleased that the Commission has put forward an ambitious proposal, which will raise the overall level of cybersecurity in the Member States and the functioning of the internal market. A harmonised regulatory framework is necessary so that undertakings who operate in the Single Market can benefit from legal clarity, as well as to ensure that the Union can play a leading role in the definition of norms on cybersecurity on the global stage.

On the issue of the scope, the rapporteur agrees with the Commission's proposal to include all products with digital elements. This comprehensive approach would provide assurance of cybersecurity compliance throughout the value chain, improving the competitiveness and the attractiveness of products manufactured in the Union. It is nonetheless necessary to simplify the current wording and refer to directly and indirectly connectable products, while excluding spare parts designed solely for the repair process, which have been in the market before this Regulation is implemented. When it comes to open source software, the Rapporteur is aware of the need to safeguard this important source of innovation and has thus put forward an amendment to ensure that developers should not be expected to comply with this Regulation if they are not receiving any financial returns for their projects. Nonetheless, open source software supplied in the framework of a commercial activity should be covered, to ensure the cybersecurity of the Union's ecosystem.

While the vast majority of products with digital elements will only have to undergo self-assessment, critical products pursuant to Article 6 will be subject to third party assessment. On this issue, the Rapporteur believes that the Regulation should be improved by providing more clarity on how often the list set out in Annex III can be amended as well as the procedures to follow after a product has been added to this list. The latter is particularly important in order to provide undertakings with adequate time to adjust. Nonetheless, the Rapporteur believes that home automation systems and products that enhance private security, such as cameras and smart locks, should constitute critical products under class I. This is because the integrity of these goods is paramount to citizens' safety and privacy.

Furthermore, the draft report foresees more involvement from stakeholders through the creation of the Expert group on Cyber Resilience. This body should be tasked to advise the Commission and to take an active role in the preparation of the delegated acts referred to in this Regulation. Thus, in order to express fully the interests of all side, the Expert group should be comprised of institutions, industry, civil society, academia and individual experts.

In addition to the aforementioned topic, the draft report stresses the need for Member States to take cybersecurity strongly into account when publicly procuring products with digital elements, and to ensure that vulnerabilities are promptly tackled.

On the issue of manufacturers' obligations, the rapporteur believes that having a set date for the expected product lifetime is inadequate to a horizontal regulation, which intends to cover a wide range of products from software to phones and industrial machineries. This is why the rapporteur believes that it is more appropriate to have manufacturers determine the lifetime of their respective products, provided that the suggested duration is compatible with reasonable consumer expectations. A flexible duration would also enable manufacturers to showcase their products and have lengthy lifetimes as an element of competitiveness. Therefore, in order to raise the awareness of the consumers to this particular matter, the regulation should also oblige

the manufacturers to clearly state the expected product lifetime on its packaging or include it in contractual agreements, and to notify the consumers when the lifetime is about to end. Furthermore, the draft report wants to put the utmost emphasis on safety. Thus, the rapporteur believes that the manufacturers should also be obliged to automatically update, when possible, safety features of their respective product. Where a manufacturer has defined an expected lifetime of under five years, it should stand ready to enter into contractual arrangements with undertakings that wish to provide services that extend a product's lifetime and disclose to them its source code. This possibility should not entail a transfer of ownership or the public disclosure of the source code.

On the matter of reporting obligations pursuant to Article 11, the Rapporteur wishes to align the timeline to the NIS2 so that there is more coherence and legal certainty for the stakeholders. In this sense, the Rapporteur suggests to report significant incidents (rather than all incidents), as well as actively exploited vulnerabilities, provided that clear protocols on how to handle such notifications securely are in place, as to avoid the spread of information concerning unpatched vulnerabilities. The Rapporteur also introduces a mechanism of voluntary reporting for other incidents, near misses and cyber threats.

However, to maximise the effect of reporting it is important to have a one-stop entity, also in order to simplify the reporting requirements for manufacturers across the Union. On this note, the Rapporteur believes that the best institution to play this role is ENISA. Therefore, in light of the increase in tasks and competence bestowed to ENISA, the Commission should modify the legislative financial statement accompanying this Regulation by providing the European Union Agency for Cybersecurity with additional posts and corresponding additional appropriations in order to fulfil the agency's additional tasks set out in this Regulation.

Additionally, an issue that is fundamental for the Rapporteur is to ensure that sufficient support is in place for undertakings to implement the requirements of this Regulation. This is particularly the case for micro, small and medium enterprises, which given their limited capabilities may find some challenges in ensuring compliance with the CRA. Therefore, the rapporteur believes that it is essential to prolong the date from which the regulation applies to 40 months. In this transition period, it should be possible for manufacturers to comply with the CRA on a voluntary basis, in order to obtain a presumption of conformity with the Radio Equipment Directive Delegated Regulation and to adapt to this Regulation ahead of its official implementation. Furthermore, the Rapporteur wants to emphasise the importance for the Union to provide support for the upskilling and reskilling of workers and ensure the availability of cybersecurity professionals, a key element for the success of this Regulation.

Moreover, as a general approach to help all stakeholders, the rapporteur calls for guidelines from the Commission to provide more specification on the actual implementation phase, thus providing more clarity to all parties involved.

Another equally pressing affair to the Rapporteur is international trade. This is why the draft report calls for the Commission to consider mutual recognition agreements with likeminded third countries, where they share comparable level of technical development and have a compatible approach concerning conformity assessment, ensuring the same level of protection as the one provided for by this Regulation. Nonetheless, it is essential that adequate monitoring of products coming from risky countries, which may contain backdoors or other vulnerabilities, is ensured: ENISA should coordinate with market surveillance authorities and perform the necessary checks on vendors who might present a higher risk profile.

Lastly, the rapporteur believes that revenues generated from the penalties should be earmarked to projects, which will raise the overall cybersecurity level across the Union, and hence be allocated to the Digital Europe Programme, supporting projects aimed at - among others - the re-skilling and upskilling of the current workforce.

ANNEX: LIST OF ENTITIES OR PERSONS FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT

The following list is drawn up on a purely voluntary basis under the exclusive responsibility of the rapporteur. The rapporteur has received input from the following entities or persons in the preparation of the report, until the adoption thereof in committee:

Entity and/or person
(ISC)2
ACEM
Airlines4Europe
Alliance for IoT and Edge Computing Innovation
Amazon
American Chamber of Commerce
ANEC
Apple

APPLiA

Associazione Italiana Internet Provider

BDI

Beuc

Bitkom

BritCham

Broadcom

BSA - The Software alliance

Business Europe

Card Payment Sweden

CEMA

Centrum für Europäische Politik

CNH

Confederation of Danish Industries (DI)

Confindustria

Cybersecurity Coalition

DEKRA

Deutsche Telekom

Developers Alliance

Digital Europe

Enedis

Engineering

Ericsson

ESMIG

ETNO

ETRMA

European Cybersecurity Organisation

European Materials Handling Federation (FEM)

Eurosmart

Federunacoma

Free Software Foundation Europe

German Insurance Association

Giesecke+Devrient

GitHub

Google

GSMA

Hanbury Strategy

Huawei

IBM

Independent Retail Europe
Information Technology Industry Council
Leaseurope
Lenovo
Mechanical Engineering Industry Association (VDMA)
MedTechEurope
Microsoft
Okta
Open Forum Europe
Orange
Orgalim
Permanent Representation of Belgium
Permanent Representation of Italy
Permanent Representation of the Netherlands
Piaggio
Privacy International
SAP
Schneider Electric
Siemens
SME United
Splunk
Technology Industries of Finland
Telefonica
TIC Council
Trellix
Twilio
Unife
Vodafone Group
Wikimedia
Worldr
Xiaomi
Zoom