



Council of the
European Union

Brussels, 23 September 2024
(OR. en)

13431/24

**Interinstitutional File:
2022/0272(COD)**

**CODEC 1804
CYBER 257
JAI 1341
DATAPROTECT 276
TELECOM 272
MI 797
CSC 539
CSCI 184
PE 218**

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - Outcome of the European Parliament's first reading and Corrigendum procedure (Strasbourg, 12 March 2024 and Strasbourg, 17 September 2024)

I. INTRODUCTION

In accordance with the provisions of Article 294 of the TFEU and the Joint Declaration on practical arrangements for the co-decision procedure¹, a number of informal contacts have taken place between the Council, the European Parliament and the Commission with a view to reaching an agreement on this legislative file at first reading.

This file was expected² to undergo the Corrigendum procedure³ in the European Parliament after adoption by the outgoing European Parliament of its position at first reading.

¹ OJ C 145, 30.6.2007, p.5.

² 10078/24.

³ Rule 251, EP Rules of Procedure.

II. VOTE

At its sitting of 12 March 2024, the European Parliament adopted amendment number 2 (without legal linguistic revision) to the Commission proposal and amendment 3 to the legislative resolution containing a statement, constituting the European Parliament's position at first reading. It reflects what had been provisionally agreed between the Institutions.

After finalisation of the adopted text by the legal linguists, the European Parliament approved on 17 September 2024 a corrigendum to the position adopted at first reading.

With this corrigendum, the Council should be able to approve the position of the European Parliament as set out in the Annex⁴ hereto, thus bringing to a close the first reading for both Institutions.

The act would then be adopted in the wording which corresponds to the European Parliament's position.

The act would then be adopted in the wording which corresponds to the Parliament's position.

⁴ The text of the corrigendum is set out in the Annex. It is presented in the form of a consolidated text, where changes to the Commission's proposal are highlighted in bold and italics. The symbol "■" indicates deleted text.

P9_TA(2024)0130

Cyber Resilience Act

European Parliament legislative resolution of 12 March 2024 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 2022¹,
 - having regard to the provisional agreement approved by the committee responsible under Rule 74(4) of its Rules of Procedure and the undertaking given by the Council representative by letter of 20 December 2023 to approve Parliament's position, in accordance with Article 294(4) of the Treaty on the Functioning of the European Union,
 - 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. Approves the joint statement by Parliament, the Council and the Commission annexed to this resolution, which will be published in the C series of the *Official Journal of the European Union*;
 3. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

¹ OJ C 100, 16.3.2023, p. 101.

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

Position of the European Parliament adopted at first reading on 12 March 2024 with a view to the adoption of Regulation (EU) 2024/... of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(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 Committee¹,

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure²,

¹ *OJ C 100, 16.3.2023, p. 101.*

² *Position of the European Parliament of 12 March 2024.*

Whereas:

- (1) ***Cybersecurity is one of the key challenges for the Union. 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 only on the Union's economy, but also on democracy as well as 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 lifecycle. 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 for products with digital elements made available on the market.*
- (3) *Relevant Union law* 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, existing Union *law* related to cybersecurity, including *Regulation (EU) 2019/881 of the European Parliament and of the Council*³ and *Directive (EU) 2022/2555 of the European Parliament and of the Council*⁴, does not directly cover mandatory requirements for the security of products with digital elements.

³ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

⁴ *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).*

- (4) While existing Union *law* 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 *businesses and organisations* to comply with a number of requirements *and obligations* for similar types of products. The cybersecurity of those products has a particularly strong cross-border dimension, as products *with digital elements* manufactured in one Member State or third 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 regulatory framework and legal certainty for users, organisations and businesses, including microenterprises and small and medium-sized enterprises as defined in the Annex to Commission Recommendation 2003/361/EC*⁵. The Union regulatory landscape should be harmonised by introducing *horizontal* cybersecurity requirements for products with digital elements.

⁵ *Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).*

In addition, legal certainty for *economic* operators and users, as well as a better harmonisation of the *internal market and proportionality for microenterprises and small and medium-sized enterprises*, creating more viable conditions for *economic* operators aiming to enter that market, should be ensured across the Union.

- (5) *As regards microenterprises and small and medium-sized enterprises, when determining the category an enterprise falls into, the provisions of the Annex to Commission Recommendation 2003/361/EC should be applied in their entirety. Therefore, when calculating the staff headcount and financial ceilings determining the enterprise categories, the provisions of Article 6 of the Annex to Commission Recommendation 2003/361/EC on establishing the data of an enterprise in consideration of specific types of enterprises, such as partner enterprises or linked enterprises, should also be applied.*

- (6) *The Commission should provide guidance to assist economic operators, particularly microenterprises and small and medium-sized enterprises, in the application of this Regulation. Such guidance should cover, inter alia, the scope of this Regulation, in particular remote data processing and its implications for free and open-source software developers, the application of the criteria used to determine support periods for products with digital elements, the interplay between this Regulation and other Union law and the concept of substantial modification.*

- (7) At Union level, various programmatic and political documents, such as the *Joint communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 16 December 2020, entitled ‘The EU’s Cybersecurity Strategy for the Digital Decade’*, the Council Conclusions of 2 December 2020 *on the cybersecurity of connected devices* and of 23 May 2022 *on the development of the European Union’s cyber posture* and the European Parliament *resolution* of 10 June 2021 *on the EU’s Cybersecurity Strategy for the Digital Decade*⁶, have called for specific Union cybersecurity requirements for digital or connected products, with several third countries introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe, 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 regulatory framework.*
- (8) 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 those products that apply horizontally.

⁶ *OJ C 67, 8.2.2022, p. 81.*

- (9) 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 to be less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or to move laterally across systems. Manufacturers should therefore ensure that all products with digital elements are designed and developed in accordance with the essential cybersecurity requirements laid down in this Regulation. ***That obligation relates to*** 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 cyber 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 products with digital elements that are only indirectly connected to other devices or networks.

- (10) By laying down cybersecurity requirements for placing on the market products with digital elements, ***it is intended that*** the cybersecurity of those products for consumers and businesses alike be enhanced. ***Those requirements will also ensure that cybersecurity is taken into account throughout supply chains, making final products with digital elements and their components more secure.*** This also includes requirements for placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitoring systems. ***Consumer products with digital elements categorised in this Regulation as important products with digital elements present a higher cybersecurity risk by performing a function which carries a significant risk of adverse effects in terms of its intensity and ability to damage the health, security or safety of users of such products, and should undergo a stricter conformity assessment procedure. This applies to such products as smart home products with security functionalities, including smart door locks, baby monitoring systems and alarm systems, connected toys and personal wearable health technology. Furthermore, the stricter conformity assessment procedures that other products with digital elements categorised in this Regulation as important or critical products with digital elements are required to undergo, will contribute to preventing potential negative impacts on consumers of the exploitation of vulnerabilities.***

- (11) ***The purpose of this Regulation is to ensure a high level of cybersecurity of products with digital elements and their integrated remote data processing solutions. Such remote data processing solutions should be defined as data processing at a distance for which the software is designed and developed by or on behalf of the manufacturer of the product with digital elements concerned*** ■ , the absence of which would prevent the product with digital elements from performing one of its functions. ***That approach ensures that such products are adequately secured in their entirety by their manufacturers, irrespective of whether data is processed or stored locally on the user’s device or remotely by the manufacturer. At the same time, processing or storage at a distance falls within the scope of this Regulation only in so far as it is necessary for a product with digital elements to perform its functions. Such processing or storage at a distance includes the situation where a mobile application requires access to an application programming interface or to a database provided by means of a service developed by the manufacturer. In such a case, the service falls within the scope of this Regulation as a remote data processing solution.***

The requirements concerning the remote data processing solutions falling within the scope of this Regulation do therefore not entail technical, operational or organisational measures aiming to manage the risks posed to the security of a manufacturer's network and information systems as a whole.

- (12) *Cloud solutions constitute remote data processing solutions within the meaning of this Regulation only if they meet the definition laid down in this Regulation. For example, cloud enabled functionalities provided by a manufacturer of smart home devices that enable users to control the device at a distance fall within the scope of this Regulation. On the other hand, websites that do not support the functionality of a product with digital elements, or cloud services designed and developed outside the responsibility of a manufacturer of a product with digital elements do not fall within the scope of this Regulation. Directive (EU) 2022/2555 applies to cloud computing services and cloud service models, such as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). Entities providing cloud computing services in the Union which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall within the scope of that Directive.*

(13) In line with the objective of this Regulation to remove obstacles to the free movement of products with digital elements, Member States should 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. Therefore, for matters harmonised by this Regulation, Member States cannot impose additional cybersecurity requirements for the making available on the market of products with digital elements. Any entity, public or private, can however establish additional requirements to those laid down in this Regulation for the procurement or use of products with digital elements for its specific purposes, and can therefore choose to use products with digital elements that meet stricter or more specific cybersecurity requirements than those applicable for the making available on the market under this Regulation. Without prejudice to Directives 2014/24/EU⁷ and 2014/25/EU⁸ of the European Parliament and of the Council, when procuring products with digital elements, which must comply with the essential cybersecurity requirements laid down in this Regulation, including those relating to vulnerability handling, Member States should ensure that such requirements are taken into consideration in the procurement process and that the manufacturers' ability to effectively apply cybersecurity measures and manage cyber threats are also taken into consideration. Furthermore, Directive (EU) 2022/2555 sets out cybersecurity risk-management measures for essential and important entities as referred to in Article 3 of that Directive that could entail supply chain security measures that require the use by such entities of products with digital elements meeting stricter cybersecurity requirements than those laid down in this Regulation. In accordance with Directive (EU) 2022/2555 and in line with its minimum harmonisation principle, Member States can therefore impose additional cybersecurity requirements for the use of ICT products by essential or important entities pursuant to that Directive in order to ensure a higher level of cybersecurity, provided that such requirements are consistent with Member States' obligations laid down in Union law. Matters not covered by this Regulation can include non-technical factors relating to products with digital elements and the

⁷ Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

⁸ Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

manufacturers thereof. Member States can therefore lay down national measures, including restrictions on products with digital elements or suppliers of such products that take account of non-technical factors. National measures relating to such factors are required to comply with Union law.

- (14) *This Regulation should be without prejudice to the Member States' responsibility for safeguarding national security, in compliance with Union law. Member States should be able to subject products with digital elements that are procured or used for national security or defence purposes to additional measures, provided that such measures are consistent with Member States' obligations laid down in Union law.*

- (15) *This Regulation applies to economic operators only in relation to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. Supply in the course of a commercial activity might be characterised not only by charging a price for a product with digital elements, but also by charging a price for technical support services where this does not serve only the recuperation of actual costs, by an intention to monetise, for instance by providing a software platform through which the manufacturer monetises other services, by requiring as a condition for use the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, or by accepting donations exceeding the costs associated with the design, development and provision of a product with digital elements. Accepting donations without the intention of making a profit should not be considered to be a commercial activity.*

- (16) *Products with digital elements provided as part of the delivery of a service for which a fee is charged solely to recover the actual costs directly related to the operation of that service, such as may be the case with certain products with digital elements provided by public administration entities, should not be considered on those grounds alone to be a commercial activity for the purposes of this Regulation. Furthermore, products with digital elements which are developed or modified by a public administration entity exclusively for its own use should not be considered to be made available on the market within the meaning of this Regulation.***

(17) *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. To foster the development and deployment of free and open-source software, in particular by microenterprises and small and medium-sized enterprises, including start-ups, individuals, not-for-profit organisations, and academic research organisations, the application of this Regulation to products with digital elements qualifying as free and open-source software supplied for distribution or use in the course of a commercial activity should take into account the nature of the different development models of software distributed and developed under free and open-source software licences.*

(18) *Free and open-source software is understood as software the source code of which is openly shared and the licensing of which provides for all rights to make it freely accessible, usable, modifiable and redistributable. Free and open-source software is developed, maintained and distributed openly, including via online platforms. In relation to economic operators that fall within the scope of this Regulation, only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity, should fall within the scope of this Regulation. The mere circumstances under which the product with digital elements has been developed, or how the development has been financed, should therefore not be taken into account when determining the commercial or non-commercial nature of that activity. More specifically, for the purposes of this Regulation and in relation to the economic operators that fall within its scope, to ensure that there is a clear distinction between the development and supply phases, the provision of products with digital elements qualifying as free and open-source software that are not monetised by their manufacturers should not be considered to be a commercial activity.*

Furthermore, the supply of products with digital elements qualifying as free and open-source software components intended for integration by other manufacturers into their own products with digital elements should be considered making available on the market only if the component is monetised by its original manufacturer. For instance, the mere fact that an open-source software product with digital elements receives financial support from manufacturers or that manufacturers contribute to the development of such a product should not in itself determine that the activity is of commercial nature. In addition, the mere presence of regular releases should not in itself lead to the conclusion that a product with digital elements is supplied in the course of a commercial activity. Finally, for the purposes of this Regulation, the development of products with digital elements qualifying as free and open-source software by not-for-profit organisations should not be considered to be a commercial activity provided that the organisation is set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives. This Regulation does not apply to natural or legal persons who contribute with source code to products with digital elements qualifying as free and open-source software that are not under their responsibility.

(19) *Taking into account the importance for cybersecurity of many products with digital elements qualifying as free and open-source software that are published, but not made available on the market within the meaning of this Regulation, legal persons who provide support on a sustained basis for the development of such products which are intended for commercial activities, and who play a main role in ensuring the viability of those products (open-source software stewards), should be subject to a light-touch and tailor-made regulatory regime. Open-source software stewards include certain foundations as well as entities that develop and publish free and open-source software in a business context, including not-for-profit entities. The regulatory regime should take account of their specific nature and compatibility with the type of obligations imposed. It should only cover products with digital elements qualifying as free and open-source software that are ultimately intended for commercial activities, such as for integration into commercial services or into monetised products with digital elements.*

For the purposes of that regulatory regime, an intention for integration into monetised products with digital elements includes cases where manufacturers that integrate a component into their own products with digital elements either contribute to the development of that component in a regular manner or provide regular financial assistance to ensure the continuity of a software product. The provision of sustained support to the development of a product with digital elements includes but is not limited to the hosting and managing of software development collaboration platforms, the hosting of source code or software, the governing or managing of products with digital elements qualifying as free and open-source software as well as the steering of the development of such products. Given that the light-touch and tailor-made regulatory regime does not subject those acting as open-source software stewards to the same obligations as those acting as manufacturers under this Regulation, they should not be permitted to affix the CE marking to the products with digital elements whose development they support.

- (20) *The sole act of hosting products with digital elements on open repositories, including through package managers or on collaboration platforms, does not in itself constitute the making available on the market of a product with digital elements. Providers of such services should be considered to be distributors only if they make such software available on the market and hence supply it for distribution or use on the Union market in the course of a commercial activity.*

(21) *In order to support and facilitate the due diligence of manufacturers that integrate free and open-source software components that are not subject to the essential cybersecurity requirements set out in this Regulation into their products with digital elements, the Commission should be able to establish voluntary security attestation programmes, either by a delegated act supplementing this Regulation or by requesting a European cybersecurity certification scheme pursuant to Article 48 of Regulation (EU) 2019/881 that takes into account the specificities of the free and open-source software development models. The security attestation programmes should be conceived in such a way that not only natural or legal persons developing or contributing to the development of a product with digital elements qualifying as free and open-source software can initiate or finance a security attestation but also third parties, such as manufacturers that integrate such products into their own products with digital elements, users, or Union and national public administrations.*

(22) *In view of the public cybersecurity objectives of this Regulation and in order to improve the situational awareness of Member States as regards the Union’s dependency on software components and in particular on potentially free and open-source software components, a dedicated administrative cooperation group (ADCO) established by this Regulation should be able to decide to jointly undertake a Union dependency assessment. Market surveillance authorities should be able to request manufacturers of categories of products with digital elements established by ADCO to submit the software bills of materials (SBOMs) that they have generated pursuant to this Regulation. In order to protect the confidentiality of SBOMs, market surveillance authorities should submit relevant information about dependencies to ADCO in an anonymised and aggregated manner.*

(23) *The effectiveness of the implementation of this Regulation will also depend on the availability of adequate cybersecurity skills. At Union level, various programmatic and political documents, including the Commission communication of 18 April 2023 on Closing the cybersecurity talent gap to boost the EU’s competitiveness, growth and resilience and the Council Conclusions of 22 May 2023 on the EU Policy on Cyber Defence acknowledged the cybersecurity skills gap in the Union and the need to address such challenges as a matter of priority, in both the public and private sectors. With a view to ensuring an effective implementation of this Regulation, Member States should ensure that adequate resources are available for the appropriate staffing of the market surveillance authorities and conformity assessment bodies to perform their tasks as laid down in this Regulation. Those measures should enhance workforce mobility in the cybersecurity field and their associated career pathways. They should also contribute to making the cybersecurity workforce more resilient and inclusive, also in terms of gender. Member States should therefore take measures to ensure that those tasks are carried out by adequately trained professionals, with the necessary cybersecurity skills.*

Similarly, manufacturers should ensure that their staff has the necessary skills to comply with their obligations as laid down in this Regulation. Member States and the Commission, in line with their prerogatives and competences and the specific tasks conferred upon them by this Regulation, should take measures to support manufacturers and in particular microenterprises and small and medium-sized enterprises, including start-ups, also in areas such as skill development, for the purposes of compliance with their obligations as laid down in this Regulation. Furthermore, as Directive (EU) 2022/2555 requires Member States to adopt policies promoting and developing training on cybersecurity and cybersecurity skills as part of their national cybersecurity strategies, Member States may also consider, when adopting such strategies, addressing the cybersecurity skills needs resulting from this Regulation, including those relating to re-skilling and up-skilling.

- (24) 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 as *referred to in Article 3 of that Directive*, including digital infrastructure providers that support core functions of the open internet, ensure internet access and provide 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 ■ 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.

(25) Regulation (EU) 2017/745 of the European Parliament and of the Council⁹ lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council¹⁰ lays down rules on *in vitro* diagnostic medical devices. *Those* 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 lifecycle approach are also covered by those Regulations. *Those* requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including *in vitro* diagnostic devices, with guidance on how to fulfil all the relevant essential requirements set out in Annex I to those Regulations with regard to cybersecurity. Products with digital elements to which either of those Regulations apply should not therefore be subject to this Regulation.

⁹ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

¹⁰ Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

- (26) *Products with digital elements that are developed or modified exclusively for national security or defence purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation. Member States are encouraged to ensure the same or a higher level of protection for those products as for those falling within the scope of this Regulation.*
- (27) Regulation (EU) 2019/2144 of the European Parliament and of the Council¹¹ 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 *cybersecurity* risks related to the entire *lifecycle* of vehicles, equipment and services in compliance with the applicable United Nations regulations on technical specifications and cybersecurity, in particular *UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system* and providing for specific conformity assessment procedures.

¹¹ Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council¹² 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 *and* equipment, including software, that *includes* obligations to protect against information security threats. ***The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation.*** Products with digital elements to which Regulation (EU) 2019/2144 applies and products certified in accordance with Regulation (EU) 2018/1139 should not therefore be subject to the essential cybersecurity requirements and conformity assessment procedures set out in this Regulation.

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

(28) This Regulation lays down horizontal cybersecurity rules which are not specific to sectors or to 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 cybersecurity requirements *set out in* 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 cybersecurity requirements set out in 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 *at least* the same level of protection as the one provided for by this Regulation. The Commission should be empowered to adopt delegated acts to *supplement* this Regulation by identifying such products and rules. For existing Union *law* where such limitation or exclusion should apply, this Regulation contains specific provisions to clarify its relation with that Union *law*.

- (29) *In order to ensure that products with digital elements made available on the market can be repaired effectively and their durability extended, an exemption should be provided for spare parts. That exemption should cover both spare parts that have the purpose of repairing legacy products made available before the date of application of this Regulation and spare parts that have already undergone a conformity assessment procedure pursuant to this Regulation.*
- (30) *Commission Delegated Regulation (EU) 2022/30¹³ specifies that a number of essential requirements set out in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU of the European Parliament and of the Council¹⁴, relating to network harm and misuse of network resources, personal data and privacy, and fraud, apply to certain radio equipment. Commission Implementing Decision C(2022) 5637 of 5 August 2022 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation lays down requirements for the development of specific standards further specifying how those essential requirements should be addressed. The essential cybersecurity requirements set out in 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. Furthermore, the essential cybersecurity requirements set out in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, when the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Implementing Decision C(2022) 5637 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation. During the transitional period for the application of this Regulation, the Commission should provide guidance to manufacturers subject to this Regulation that*

¹³ *Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (OJ L 7, 12.1.2022, p. 6).*

¹⁴ *Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).*

are also subject to Delegated Regulation (EU) 2022/30 to facilitate the demonstration of compliance with the two Regulations.

(31) ***Directive (EU) 2024/... of the European Parliament and of the Council***¹⁵⁺ 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 the placing on the market of the product, 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.

¹⁵ ***Directive (EU) .../... of the European Parliament and of the Council of... on ... (OJ ..., ELI: ...).***

⁺ ***OJ: Please insert in the text the number of the Directive contained in document (2022/0302(COD)) and insert the number, date, title and OJ reference of that Directive in the footnote.***

(32) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council¹⁶, including to provisions *relating to* 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 of 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 established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and Union data protection law should also be created in the area of market surveillance and enforcement.

¹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

To that end, national market surveillance authorities designated under this Regulation should cooperate with authorities supervising the application of Union data protection law. The latter should also have access to information relevant for accomplishing their tasks.

- (33) To the extent that their products fall within the scope of this Regulation, **providers** of European Digital Identity Wallets as referred to in Article 5a(2) of Regulation (EU) No 910/2014 **of the European Parliament and of the Council**¹⁷, should comply with both the horizontal essential cybersecurity requirements **set out in** this Regulation and the specific security requirements **set out in** Article 5a of Regulation (EU) No 910/2014. In order to facilitate compliance, wallet **providers** should be able to demonstrate the compliance of European Digital Identity Wallets with the requirements set out **in this Regulation and in Regulation (EU) No 910/2014**, respectively, by certifying their products under a European cybersecurity certification scheme established under Regulation (EU) 2019/881 and for which the Commission **has** specified, **by means of delegated acts**, a presumption of conformity for this Regulation, in so far as the certificate, or parts thereof, covers those requirements.

¹⁷ **Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).**

(34) *When integrating components sourced from third parties in products with digital elements during the design and development phase, manufacturers should, in order to ensure that the products are designed, developed and produced in accordance with the essential cybersecurity requirements set out in this Regulation, exercise due diligence with regard to those components, including free and open-source software components that have not been made available on the market. The appropriate level of due diligence depends on the nature and the level of cybersecurity risk associated with a given component, and should, for that purpose, take into account one or more of the following actions: verifying, as applicable, that the manufacturer of a component has demonstrated conformity with this Regulation, including by checking if the component already bears the CE marking; verifying that a component receives regular security updates, such as by checking its security updates history; verifying that a component is free from vulnerabilities registered in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555 or other publicly accessible vulnerability databases; or carrying out additional security tests.*

The vulnerability handling obligations set out in this Regulation, which manufacturers have to comply with when placing a product with digital elements on the market and for the support period, apply to products with digital elements in their entirety, including to all integrated components. Where, in the exercise of due diligence, the manufacturer of the product with digital elements identifies a vulnerability in a component, including in a free and open-source component, it should inform the person or entity manufacturing or maintaining the component, address and remediate the vulnerability, and, where applicable, provide the person or entity with the applied security fix.

- (35) *Immediately after the transitional period for the application of this Regulation, a manufacturer of a product with digital elements that integrates one or several components sourced from third parties which are also subject to this Regulation may not be able to verify, as part of its due diligence obligation, that the manufacturers of those components have demonstrated conformity with this Regulation by checking, for instance, if the components already bear the CE marking. This may be the case where the components have been integrated before this Regulation becomes applicable to the manufacturers of those components. In such a case, a manufacturer integrating such components should exercise due diligence through other means.*

- (36) 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 or use of a product with digital elements which does not comply with this Regulation, including its prototypes, provided that the product is presented with a visible sign clearly indicating that the product does not comply with this Regulation and is not to be made available on the market until it does so.***

(37) In order to ensure that manufacturers can release software for testing purposes before subjecting their products with digital elements to conformity assessment, Member States should not prevent the making available of unfinished software, such as alpha versions, beta versions or release candidates, ***provided that the unfinished*** software is made available ***only*** for the time necessary to test it and gather feedback. Manufacturers should ensure that software made available under *those* conditions is released ***only*** 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 ***laid down in*** 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.

- (38) In order to ensure that products with digital elements, when placed on the market, do not pose cybersecurity risks to persons and organisations, essential cybersecurity requirements should be set out for such products. ***Those essential cybersecurity requirements, including vulnerability management handling requirements, apply to each individual product with digital elements when placed on the market, irrespective of whether the product with digital elements is manufactured as an individual unit or in series. For example, for a product type, each individual product with digital elements should have received all security patches or updates available to address relevant security issues when it is placed on the market. Where products with digital elements are subsequently modified, by physical or digital means, in a way that is not foreseen by the manufacturer in the initial risk assessment and that may imply that they no longer meet the relevant essential cybersecurity requirements, the modification should be considered to be substantial. For example, repairs could be assimilated to maintenance operations provided that they do not modify a product with digital elements already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended purpose for which the product has been assessed may be changed.***

(39) *As is the case for physical repairs or modifications, a product with digital elements should be considered to be substantially modified by a software change where the software update modifies the intended purpose of that product and those changes were not foreseen by the manufacturer in the initial risk assessment, or where the nature of the hazard has changed or the level of cybersecurity risk has increased because of the software update, and the updated version of the product is made available on the market. Where a security update which is designed to decrease the level of cybersecurity risk of a product with digital elements does not modify the intended purpose of a product with digital elements, it is not considered to be a substantial modification. This usually includes situations where a security update entails only minor adjustments of the source code. For example, this could be the case where a security update addresses a known vulnerability, including by modifying functions or the performance of a product with digital elements for the sole purpose of decreasing the level of cybersecurity risk. Similarly, a minor functionality update, such as a visual enhancement or the addition of new pictograms or languages to the user interface, should not generally be considered to be a substantial modification.*

Conversely, where a feature update modifies the original intended functions or the type or performance of a product with digital elements and meets the above criteria, it should be considered to be a substantial modification, as the addition of new features typically leads to a broader attack surface, thereby increasing the cybersecurity risk. For example, this could be the case where a new input element is added to an application, requiring the manufacturer to ensure adequate input validation. In assessing whether a feature update is considered to be a substantial modification it is not relevant whether it is provided as a separate update or in combination with a security update. The Commission should issue guidance on how to determine what constitutes a substantial modification.

(40) *Taking into account the iterative nature of software development, manufacturers that have placed subsequent versions of a software product on the market as a result of a subsequent substantial modification of that product should be able to provide security updates for the support period only for the version of the software product that they have last placed on the market. They should be able to do so only if the users of the relevant previous product versions have access to the product version last placed on the market free of charge and do not incur additional costs to adjust the hardware or software environment in which they operate the product. This could, for instance, be the case where a desktop operating system upgrade does not require new hardware, such as a faster central processing unit or more memory. Nonetheless, the manufacturer should continue to comply, for the support period, with other vulnerability-handling requirements, such as having a policy on coordinated vulnerability disclosure or measures in place to facilitate the sharing of information about potential vulnerabilities for all subsequent substantially modified versions of the software product placed on the market.*

Manufacturers should be able to provide minor security or functionality updates that do not constitute a substantial modification only for the latest version or sub-version of a software product that has not been substantially modified. At the same time, where a hardware product, such as a smartphone, is not compatible with the latest version of the operating system it was originally delivered with, the manufacturer should continue to provide security updates at least for the latest compatible version of the operating system for the support period.

- (41) In line with the commonly established concept of substantial modification for products regulated by Union harmonisation legislation, where a substantial modification occurs that may affect the compliance of a product *with digital elements* 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, a change that might lead to a substantial modification should be notified to the third party.

- (42) Where a product with digital elements is subject to ‘refurbishment’, ‘maintenance’ and ‘repair’ as defined in Article 2, points (18), (19) and (20), of Regulation ***(EU) 2024/1781 of the European Parliament and of the Council¹⁸***, this does not necessarily lead to a substantial modification of the product, for instance if the intended ***purpose*** and functionalities are not changed and the level of risk remains unaffected. However, an upgrade of a product ***with digital elements*** by the manufacturer might lead to changes in the design and development of that product and might therefore affect its intended ***purpose*** and compliance with the requirements set out in this Regulation.

¹⁸ ***Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (OJ L, 2024/1781, 28.6.2024, ELI: <http://data.europa.eu/eli/reg/2024/1781/oj>).***

- (43) Products with digital elements should be considered to be **important** if the negative impact of the exploitation of potential vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality **or a function carrying a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data**. In particular, vulnerabilities in products with digital elements that have a cybersecurity-related functionality, such as **boot managers**, can lead to a propagation of security issues throughout the supply chain. The severity of the impact of an incident may also increase **where the product primarily performs a central system function, including network management, configuration control, virtualisation or processing of personal data**.

- (44) *Certain categories of* products with digital elements should be subject to stricter conformity assessment procedures, while keeping a proportionate approach. For that purpose, *important* products with digital elements should be divided into two classes, reflecting the level of cybersecurity risk linked to those categories of products. An incident involving *important* products *with digital elements that fall under* class II might lead to greater negative impacts than an incident involving *important* products *with digital elements* that fall under class I, for instance due to the nature of their cybersecurity-related function or *the performance of another function which carries a significant risk of adverse effects*. *As an indication of such greater negative impacts, products with digital elements that fall under class II could either perform a cybersecurity-related functionality or another function which carries a significant risk of adverse effects that is higher than for those listed in class I, or meet both of the aforementioned criteria. Important products with digital elements that fall under class II should therefore be subject to a stricter conformity assessment procedure.*

(45) **Important** products with digital elements referred to in this Regulation should be understood as products which have the core functionality of **a category of important products with digital elements** that is **set out** in this Regulation. For example, this Regulation **sets out categories of important products with digital elements** which are defined by their core functionality as **firewalls or intrusion detection or prevention systems** in class II. As a result, **firewalls and intrusion detection or prevention systems** are subject to mandatory third-party conformity assessment. This is not the case for other products **with digital elements** not **categorised as important products with digital elements** which may integrate **firewalls or intrusion detection or prevention systems**. The Commission should adopt **an implementing act** to specify the **technical description** of the categories **of important products with digital elements that fall** under classes I and II as set out in **this Regulation**.

(46) *The categories of critical products with digital elements set out in this Regulation have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation. Furthermore, those categories of products with digital elements are considered to be critical dependencies for essential entities referred to in Article 3(1) of Directive (EU) 2022/2555. The categories of critical products with digital elements set out in an annex to this Regulation, due to their criticality, already widely use various forms of certification, and are also covered by the European Common Criteria-based cybersecurity certification scheme (EUCC) set out in Commission Implementing Regulation (EU) 2024/482¹⁹. Therefore, in order to ensure a common adequate cybersecurity protection of critical products with digital elements in the Union, it could be adequate and proportionate to subject such categories of product, by means of a delegated act, to mandatory European cybersecurity certification where a relevant European cybersecurity certification scheme covering those products is already in place and an assessment of the potential market impact of the envisaged mandatory certification has been carried out by the Commission.*

¹⁹ *Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).*

That assessment should consider both the supply and demand side, including whether there is sufficient demand for the products with digital elements concerned from both Member States and users for European cybersecurity certification to be required, as well as the purposes for which the products with digital elements are intended to be used, including the critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555. The assessment should also analyse the potential effects of the mandatory certification on the availability of those products on the internal market and the capabilities and the readiness of the Member States for the implementation of the relevant European cybersecurity certification schemes.

(47) Delegated acts requiring mandatory European cybersecurity certification should determine the products with digital elements that have the core functionality of a category of critical products with digital elements set out in this Regulation that are to be subject to mandatory certification, as well as the required assurance level, which should be at least ‘substantial’. The required assurance level should be proportionate to the level of cybersecurity risk associated with the product with digital elements. For instance, where the product with digital elements has the core functionality of a category of critical products with digital elements set out in this Regulation and is intended for the use in a sensitive or critical environment, such as products intended for the use of essential entities referred to in Article 3(1) of Directive (EU) 2022/2555, it may require the highest assurance level.

(48) *In order to ensure a common adequate cybersecurity protection in the Union of products with digital elements that have the core functionality of a category of critical products with digital elements set out in this Regulation, the Commission should also be empowered to adopt delegated acts to amend this Regulation by adding or withdrawing categories of critical products with digital elements for which manufacturers could be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with this Regulation. A new category of critical products with digital elements can be added to those categories if there is a critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555 or, if affected by incidents or when containing exploited vulnerabilities, this could lead to disruptions of critical supply chains. When assessing the need for adding or withdrawing categories of critical products with digital elements by means of a delegated act, the Commission should be able to take into account whether the Member States have identified at national level products with digital elements that have a critical role for the resilience of essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555 and which increasingly face supply chain cyberattacks, with potential serious disruptive effects.*

Furthermore, the Commission should be able to take into account the outcome of the Union level coordinated security risk assessment of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555.

- (49)** *The Commission should ensure that a wide range of relevant stakeholders are consulted in a structured and regular manner when preparing measures for the implementation of this Regulation. This should particularly be the case where the Commission assesses the need for potential updates to the lists of categories of important or critical products with digital elements, where relevant manufacturers should be consulted and their views taken into account in order to analyse the cybersecurity risks as well as the balance of costs and benefits of designating such categories of products as important or critical.*

- (50) 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 relevant Union *harmonisation* legislation *other than this Regulation*. If no Union harmonisation legislation *other than this Regulation* is applicable, they should be subject to Regulation *(EU) 2023/988 of the European Parliament and of the Council*²⁰. 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 laid down in Union harmonisation legislation *other than this Regulation* within the meaning of Article 3, point (27), of Regulation *(EU) 2023/988*.

²⁰ *Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).*

(51) Products with digital elements classified as high-risk AI systems pursuant to Article 6 of Regulation **(EU) 2024/1689 of the European Parliament and of the Council**²¹ which fall within the scope of this Regulation should comply with the essential cybersecurity requirements set out in this Regulation. Where those high-risk AI systems fulfil the essential cybersecurity requirements set out in this Regulation, they should be deemed **to comply** with the cybersecurity requirements set out in Article 15 of Regulation **(EU) 2024/1689** in so far as those requirements are covered by the EU declaration of conformity or parts thereof issued under this Regulation. ***For that purpose, the assessment of the cybersecurity risks associated with a product with digital elements classified as a high-risk AI system pursuant to Regulation (EU) 2024/1689 that is to be taken into account during the planning, design, development, production, delivery and maintenance phases of such product, as required under this Regulation, should take into account risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights, in accordance with Regulation (EU) 2024/1689.*** As regards the conformity assessment procedures relating to the essential cybersecurity requirements for a product with digital elements ***that falls within the scope of*** this Regulation and that is classified as a high-risk AI system, Article 43 of Regulation **(EU) 2024/1689** should apply as a rule instead of the ***relevant*** provisions of this Regulation. However, that rule should not result in a reduction of the necessary level of assurance for ***important or*** critical products with digital elements ***as referred to in*** this Regulation. Therefore, by way of derogation from that rule, high-risk AI systems that fall within the scope of Regulation **(EU) 2024/1689** which are also ***important or*** critical products with digital elements ***as referred to in*** this Regulation and to which the conformity assessment procedure based on internal control referred to in Annex VI ***to*** Regulation **(EU) 2024/1689** applies, should be subject to the conformity assessment ***procedures provided for in*** this Regulation in so far as the essential cybersecurity

²¹ ***Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).***

requirements set out in this Regulation are concerned. In such a case, for all the other aspects covered by Regulation **(EU) 2024/1689** the *relevant* provisions on conformity assessment based on internal control set out in Annex VI to *that* Regulation should apply.

(52) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential cybersecurity requirements ***applicable to such products***. Those essential cybersecurity requirements should be without prejudice to the ***Union level*** coordinated ***security*** risk assessments of critical supply chains ***provided for in*** Article 22 of Directive ***(EU) 2022/2555***, which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, ***they*** should be without prejudice to the Member States' prerogative 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 ***Commission*** Recommendation (EU) 2019/534²², in the ***EU*** coordinated risk assessment of ***the cybersecurity of*** 5G networks and in the EU Toolbox on 5G cybersecurity agreed by the ***Cooperation Group established pursuant to Article 14 of*** Directive ***(EU) 2022/2555***.

²² ***Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).***

(53) ***Manufacturers of products falling within the scope of Regulation (EU) 2023/1230 of the European Parliament and of the Council²³ which are also products with digital elements within the meaning of this Regulation should comply with both the essential cybersecurity requirements set out in this Regulation and the essential health and safety requirements set out in Regulation (EU) 2023/1230. The essential cybersecurity requirements set out in this Regulation and certain essential requirements set out in Regulation (EU) 2023/1230 might address similar cybersecurity risks. Therefore, the compliance with the essential cybersecurity requirements set out in this Regulation could facilitate the compliance with the essential requirements that also cover certain cybersecurity risks as set out in Regulation (EU) 2023/1230, and in particular those regarding the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. Such synergies have to be demonstrated by the manufacturer, for instance by applying, where available, harmonised standards or other technical specifications covering relevant essential cybersecurity requirements following a risk assessment covering those cybersecurity risks. The manufacturer should also follow the applicable conformity assessment procedures set out in this Regulation and in Regulation (EU) 2023/1230. The Commission and the European Standardisation Organisations, in the preparatory work supporting the implementation of this Regulation and of Regulation (EU) 2023/1230 and the related standardisation processes, should promote consistency in how the cybersecurity risks are to be assessed and in how those risks are to be covered by harmonised standards with regard to the relevant essential requirements. In particular, the Commission and the European Standardisation Organisations should take into account this Regulation in the preparation and development of harmonised standards to facilitate the implementation of Regulation (EU) 2023/1230 as regards in particular the cybersecurity aspects related to the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. The Commission should provide guidance to support manufacturers subject to this Regulation that are also subject to Regulation (EU) 2023/1230, in particular to facilitate the demonstration of compliance***

²³ ***Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (OJ L 165, 29.6.2023, p. 1).***

with relevant essential requirements set out in this Regulation and in Regulation (EU) 2023/1230.

- (54) In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as ***during the time the product with digital elements is expected to be in use***, it is necessary to lay down essential cybersecurity requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential cybersecurity requirements related to vulnerability handling ***throughout the support period***, they should determine which other essential cybersecurity requirements related to the product properties are relevant for the type of product ***with digital elements concerned***. For that purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential cybersecurity requirements in order to ***make available their products with digital elements 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 European or international standards***.

(55) *Where certain essential cybersecurity requirements are not applicable to a product with digital elements, the manufacturer should include a clear justification in the cybersecurity risk assessment included in the technical documentation. This could be the case where an essential cybersecurity requirement is incompatible with the nature of a product with digital elements. For example, the intended purpose of a product with digital elements may require the manufacturer to follow widely recognised interoperability standards even if its security features are no longer considered to be state of the art. Similarly, other Union law requires manufacturers to apply specific interoperability requirements. Where an essential cybersecurity requirement is not applicable to a product with digital elements, but the manufacturer has identified cybersecurity risks in relation to that essential cybersecurity requirement, it should take measures to address those risks by other means, for instance by limiting the intended purpose of the product to trusted environments or by informing the users about those risks.*

(56) *One of the most important measures for users to take in order to protect their products with digital elements from cyberattacks is to install the latest available security updates as soon as possible. Manufacturers should therefore design their products and put in place processes to ensure that products with digital elements include functions that enable the notification, distribution, download and installation of security updates automatically, in particular in the case of consumer products. They should also provide the possibility to approve the download and installation of the security updates as a final step. Users should retain the ability to deactivate automatic updates, with a clear and easy-to-use mechanism, supported by clear instructions on how users can opt out. The requirements relating to automatic updates as set out in an annex to this Regulation are not applicable to products with digital elements primarily intended to be integrated as components into other products. They also do not apply to products with digital elements for which users would not reasonably expect automatic updates, including products with digital elements intended to be used in professional ICT networks, and especially in critical and industrial environments where an automatic update could cause interference with operations.*

Irrespective of whether a product with digital elements is designed to receive automatic updates or not, its manufacturer should inform users about vulnerabilities and make security updates available without delay. Where a product with digital elements has a user interface or similar technical means allowing direct interaction with its users, the manufacturer should make use of such features to inform users that their product with digital elements has reached the end of the support period. Notifications should be limited to what is necessary in order to ensure the effective reception of this information and should not have a negative impact on the user experience of the product with digital elements.

- (57) *To improve the transparency of vulnerability handling processes and to ensure that users are not required to install new functionality updates for the sole purpose of receiving the latest security updates, manufacturers should ensure, where technically feasible, that new security updates are provided separately from functionality updates.*

(58) *The joint communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 20 June 2023 entitled ‘European Economic Security Strategy’ stated that 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. Dependencies on high-risk suppliers of products with digital elements may pose a strategic risk that needs to be addressed at Union level, especially where the products with digital elements are intended for the use by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555. Such risks may be linked, but not limited, 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 where a third country engages in economic espionage or irresponsible state behaviour in cyberspace and its legislation allows 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 mechanisms, due process or the right to appeal to an independent court or tribunal.*

When determining the significance of a cybersecurity risk within the meaning of this Regulation, the Commission and the market surveillance authorities, as per their responsibilities set out in this Regulation, should also consider non-technical risk factors, in particular those established as a result of Union level coordinated security risk assessments of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555.

- (59) *For the purpose of ensuring the security of products with digital elements after their placing on the market, manufacturers should determine the support period, which should reflect the time the product with digital elements is expected to be in use. In determining a support period, a manufacturer should take into account in particular reasonable user expectations, the nature of the product, as well as relevant Union law determining the lifetime of products with digital elements. Manufacturers should also be able to take into account other relevant factors. Criteria should be applied in a manner that ensures proportionality in the determination of the support period. Upon request, a manufacturer should provide market surveillance authorities with the information that was taken into account to determine the support period of a product with digital elements.*

(60) *The support period for which the manufacturer ensures the effective handling of vulnerabilities should be no less than five years, unless the lifetime of the product with digital elements is less than five years, in which case the manufacturer should ensure the vulnerability handling for that lifetime. Where the time the product with digital elements is reasonably expected to be in use is longer than five years, as is often the case for hardware components such as motherboards or microprocessors, network devices such as routers, modems or switches, as well as software, such as operating systems or video-editing tools, manufacturers should accordingly ensure longer support periods. In particular, products with digital elements intended for use in industrial settings, such as industrial control systems, are often in use for significantly longer periods of time. A manufacturer should be able to define a support period of less than five years only where this is justified by the nature of the product with digital elements concerned and where that product is expected to be in use for less than five years, in which case the support period should correspond to the expected use time. For instance, the lifetime of a contact tracing application intended for use during a pandemic could be limited to the duration of the pandemic.*

Moreover, some software applications can by nature only be made available on the basis of a subscription model, in particular where the application becomes unavailable to the user and is consequently not in use anymore once the subscription expires.

- (61) When products with digital elements reach the end of their support periods, in order to ensure that vulnerabilities can be handled after the end of the support period, manufacturers should consider releasing the source code of such products with digital elements either to other undertakings which commit to extending the provision of vulnerability handling services or to the public. Where manufacturers release the source code to other undertakings, they should be able to protect the ownership of the product with digital elements and prevent the dissemination of the source code to the public, for example through contractual arrangements.*

(62) *In order to ensure that manufacturers across the Union determine similar support periods for comparable products with digital elements, ADCO should publish statistics on the average support periods determined by manufacturers for categories of products with digital elements and issue guidance indicating appropriate support periods for such categories. In addition, with a view to ensuring a harmonised approach across the internal market, the Commission should be able to adopt delegated acts to specify minimum support periods for specific product categories where the data provided by market surveillance authorities suggests that the support periods determined by manufacturers are either systematically not in line with the criteria for determining the support periods as laid down in this Regulation or that manufacturers in different Member States unjustifiably determine different support periods.*

- (63) *Manufacturers should set up a single point of contact that enables users to communicate easily with them, including for the purpose of reporting on and receiving information about the vulnerabilities of the product with digital element. They should make the single point of contact easily accessible for users and clearly indicate its availability, keeping this information up to date. Where manufacturers choose to offer automated tools, e.g. chat boxes, they should also offer a phone number or other digital means of contact, such as an email address or a contact form. The single point of contact should not rely exclusively on automated tools.*
- (64) *Manufacturers should make their products with digital elements available on the market with a secure by default configuration and provide security updates to users free of charge. Manufacturers should only be able to deviate from the essential cybersecurity requirements in relation to tailor-made products that are fitted to a particular purpose for a particular business user and where both the manufacturer and the user have explicitly agreed to a different set of contractual terms.*

(65) Manufacturers should notify simultaneously via the single reporting platform both the Computer Security Incident Response Team (CSIRT) designated as coordinator as well as ENISA of actively exploited vulnerabilities contained in products with digital elements, as well as severe incidents having an impact on the security of those products. The notifications should be submitted using the electronic notification end-point of a CSIRT designated as coordinator and should be simultaneously accessible to ENISA.

(66) *Manufacturers should notify actively exploited vulnerabilities to ensure that the CSIRTs designated as coordinators, and ENISA, have an adequate overview of such vulnerabilities and* are provided with the information necessary to fulfil their tasks *as set out in Directive (EU) 2022/2555* and raise the overall level of cybersecurity of essential and important entities *as referred to in Article 3 of that Directive, as well as* to ensure the effective functioning of market surveillance authorities **■** . 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 to be a threat to the functioning of the internal market. *ENISA should, in agreement with the manufacturer, disclose* fixed vulnerabilities to the European vulnerability database established *pursuant to Article 12(2) of Directive (EU) 2022/2555. The European* vulnerability database *will assist manufacturers in detecting known exploitable vulnerabilities in their products, in order to ensure that secure products are made available on the market.*

- (67) Manufacturers should also **notify** any **severe** incident having an impact on the security of the product with digital elements **to the CSIRT** designated **as coordinator and** ENISA **█** . In order to ensure that users can react quickly to **severe** 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 **cybersecurity** risks, by reaching out to the users directly.

(68) *Actively exploited vulnerabilities concern instances where a manufacturer establishes that a security breach affecting its users or any other natural or legal persons has resulted from a malicious actor making use of a flaw in one of the products with digital elements made available on the market by the manufacturer. Examples of such vulnerabilities could be weaknesses in a product’s 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 notification. Severe incidents having an impact on the security of the product with digital elements, on the other hand, refer to situations where a cybersecurity incident affects the development, production or maintenance processes of the manufacturer in such a way that it could result in an increased cybersecurity risk for users or other persons. Such a severe incident could include a situation where an attacker has successfully introduced malicious code into the release channel via which the manufacturer releases security updates to users.*

(69) *To ensure that notifications can be disseminated quickly to all relevant CSIRTs designated as coordinators and to enable manufacturers to submit a single notification at each stage of the notification process, a single reporting platform with national electronic notification end-points should be established by ENISA. The day-to-day operations of the single reporting platform should be managed and maintained by ENISA. The CSIRTs designated as coordinators should inform their respective market surveillance authorities about notified vulnerabilities or incidents. The single reporting platform should be designed in such a way that it ensures the confidentiality of notifications, in particular as regards vulnerabilities for which a security update is not yet available. In addition, ENISA should put in place procedures to handle information in a secure and confidential manner. 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 established pursuant to Article 14 of Directive (EU) 2022/2555.*

(70) *In exceptional circumstances and in particular upon request by the manufacturer, the CSIRT designated as coordinator initially receiving a notification should be able to decide to delay its dissemination to the other relevant CSIRTs designated as coordinators via the single reporting platform where this can be justified on cybersecurity-related grounds and for a period of time that is strictly necessary. The CSIRT designated as coordinator should immediately inform ENISA about the decision to delay and on which grounds, as well as when it intends to disseminate further. The Commission should develop, through a delegated act, specifications on the terms and conditions for when cybersecurity-related grounds could be applied and should cooperate with the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555, and ENISA in preparing the draft delegated act. Examples of cybersecurity-related grounds include an ongoing coordinated vulnerability disclosure procedure or situations in which a manufacturer is expected to provide a mitigating measure shortly and the cybersecurity risks of an immediate dissemination via the single reporting platform outweigh its benefits. If requested by the CSIRT designated as coordinator, ENISA should be able to support that CSIRT on the application of cybersecurity-related grounds in relation to delaying the dissemination of the notification based on the information ENISA has received from that CSIRT on the decision to withhold a notification on those cybersecurity-related grounds. Furthermore, in particularly exceptional circumstances, ENISA should not receive all the details of a notification of an actively exploited vulnerability in a simultaneous manner. This would be the case when the manufacturer marks in its notification that the notified vulnerability has been actively exploited by a malicious actor and that, according to the information available, it has been exploited in no other Member State than the one of the CSIRT designated as coordinator to which the manufacturer has notified the vulnerability, when any immediate further dissemination of the notified vulnerability would likely result in the supply of information the disclosure of which would be contrary to the essential interests of that Member State, or when the notified vulnerability poses an imminent high cybersecurity risk stemming from the further dissemination. In such cases, ENISA will only receive simultaneous access to the information that a notification was made by the manufacturer, general information about the product with digital elements concerned, the information about the general nature of the exploit and information about the fact*

that those security grounds were raised by the manufacturer and that the full content of the notification is therefore withheld. The full notification should then be made available to ENISA and other relevant CSIRTs designated as coordinators when the CSIRT designated as coordinator initially receiving the notification finds that those security grounds, reflecting particularly exceptional circumstances as established in this Regulation, cease to exist. Where, based on the information available, ENISA considers that there is a systemic risk affecting the security of the internal market, ENISA should recommend to the recipient CSIRT to disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.

(71) *When manufacturers notify an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, they should indicate how sensitive they consider the notified information to be. The CSIRT designated as coordinator initially receiving the notification should take this information into account when assessing whether the notification gives rise to exceptional circumstances that justify a delay in the dissemination of the notification to the other relevant CSIRTs designated as coordinators based on justified cybersecurity-related grounds. It should also take that information into account when assessing whether the notification of an actively exploited vulnerability gives rise to particularly exceptional circumstances that justify that the full notification is not made available simultaneously to ENISA. Finally, CSIRTs designated as coordinators should be able to take that information into account when determining appropriate measures to mitigate the risks stemming from such vulnerabilities and incidents.*

(72) *In order to simplify the reporting of information required under this Regulation, in consideration of other complementary reporting requirements laid down in Union law, such as Regulation (EU) 2016/679, Regulation (EU) 2022/2554 of the European Parliament and of the Council²⁴, Directive 2002/58/EC of the European Parliament and of the Council²⁵ and Directive (EU) 2022/2555, as well as to decrease the administrative burden for entities, Member States are encouraged to consider providing at national level single entry points for such reporting requirements. The use of such national single entry points for the reporting of security incidents under Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to the independence of the authorities referred to therein. When establishing the single reporting platform referred to in this Regulation, ENISA should take into account the possibility for the national electronic notification end-points referred to in this Regulation to be integrated into national single entry points that may also integrate other notifications required under Union law.*

²⁴ *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).*

²⁵ *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37).*

- (73) *When establishing the single reporting platform referred to in this Regulation and in order to benefit from past experience, ENISA should consult other Union institutions or agencies that are managing platforms or databases subject to stringent security requirements, such as the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). ENISA should also analyse potential complementarities with the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555.*
- (74) *Manufacturers and other natural and legal persons should be able to notify to a CSIRT designated as coordinator or ENISA, on a voluntary basis, any vulnerability contained in a product with digital elements, cyber threats that could affect the risk profile of a product with digital elements, any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident.*

(75) Member States should aim to address, to the extent possible, the challenges faced by vulnerability researchers, including their potential exposure to criminal liability, in accordance with national law. Given that natural and legal persons researching vulnerabilities could in some Member States be exposed to criminal and civil liability, Member States are encouraged to adopt guidelines as regards the non-prosecution of information security researchers and an exemption from civil liability for their activities.

(76) 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 coordinators 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. **Moreover, manufacturers should also consider publishing their security policies in machine-readable format.** 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. This refers to so-called ‘bug bounty programmes’.

- (77) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up an ***SBOM***. ***An SBOM*** can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, ***in particular*** it helps manufacturers and users to track known newly emerged vulnerabilities and ***cybersecurity*** risks. It is of particular importance that manufacturers ensure that their products ***with digital elements*** do not contain vulnerable components developed by third parties. ***Manufacturers should not be obliged to make the SBOM public.***

(78) *Under the new complex business models linked to online sales, a business operating online can provide a variety of services. Depending on the nature of the services provided in relation to a given product with digital elements, the same entity may fall within different categories of business models or economic operators. Where an entity provides only online intermediation services for a given product with digital elements and is merely a provider of an online marketplace as defined in Article 3, point (14), of Regulation (EU) 2023/988, it does not qualify as one of the types of economic operator defined in this Regulation. Where the same entity is a provider of an online marketplace and also acts as an economic operator as defined in this Regulation for the sale of particular products with digital elements, it should be subject to the obligations set out in this Regulation for that type of economic operator. For instance, if the provider of an online marketplace also distributes a product with digital elements, then, with respect to the sale of that product, it would be considered to be a distributor.*

Similarly, if the entity in question sells its own branded products with digital elements, it would qualify as a manufacturer and would thus have to comply with the applicable requirements for manufacturers. Also, some entities can qualify as fulfilment service providers as defined in Article 3, point (11), of Regulation (EU) 2019/1020 of the European Parliament and of the Council²⁶ if they offer such services. Such cases would need to be assessed on a case-by-case basis. 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 help ensure that products with digital elements purchased through online marketplaces comply with the cybersecurity requirements laid down in this Regulation.

²⁶ *Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).*

(79) In order to facilitate assessment of conformity with the requirements laid down in 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 cybersecurity requirements set out in 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 Council²⁷. ***That*** Regulation provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements set out in this Regulation. ***The standardisation process should ensure a balanced representation of interests and effective participation of civil society stakeholders, including consumer organisations. International standards that are in line with the level of cybersecurity protection aimed for by the essential cybersecurity requirements set out in this Regulation should also be taken into account, in order to facilitate the development of harmonised standards and the implementation of this Regulation, as well as to facilitate compliance for companies, in particular microenterprises and small and medium-sized enterprises and those operating globally.***

²⁷ Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(80) *The timely development of harmonised standards during the transitional period for the application of this Regulation and their availability before the date of application of this Regulation will be particularly important for its effective implementation. This is, in particular, the case for important products with digital elements that fall under class I. The availability of harmonised standards will enable manufacturers of such products to perform the conformity assessments via the internal control procedure and can therefore avoid bottlenecks and delays in the activities of conformity assessment bodies.*

(81) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, *ICT* processes and *ICT* services. European cybersecurity certification schemes *provide a common framework of trust for users to use* products with digital elements *that fall within the scope of* 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 *European* cybersecurity scheme pursuant to Regulation (EU) 2019/881 *that* has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential cybersecurity requirements *set out in* this Regulation in so far as the *European* 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, *including when preparing the Union rolling work programme in accordance with Regulation (EU) 2019/881.*

*Where there is a need for a new scheme covering products with digital elements, including in order to facilitate compliance with this Regulation, the Commission can request ENISA to prepare candidate schemes in accordance with Article 48 of Regulation (EU) 2019/881. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential cybersecurity requirements **and conformity assessment procedures** as set out in this Regulation and facilitate compliance with this Regulation. **For European cybersecurity certification schemes that enter into force before the entry into force of this Regulation, further specifications may be needed on detailed aspects of how a presumption of conformity can apply.** The Commission, **by means of delegated acts**, should be empowered to specify **under which conditions** the European cybersecurity certification schemes **■** can be used to demonstrate conformity with the essential cybersecurity requirements set out in this Regulation. Furthermore, **■** to avoid undue administrative burdens, **there** should **be no** obligation for manufacturers to carry out a third-party conformity assessment as provided **for in** this Regulation for corresponding requirements **where a European cybersecurity certificate has been issued under such European cybersecurity certification schemes at least at level ‘substantial’.***

- (82) Upon entry into force of Implementing Regulation (EU) 2024/482 which concerns **■** products *that fall within the scope of* this Regulation, such as hardware security modules and microprocessors, the Commission *should be able to* specify, by means of *a delegated* act, how the EUCC provides a presumption of conformity with the essential cybersecurity requirements as *set out* in this Regulation or parts thereof. Furthermore, such *a delegated* act may specify how a certificate issued under the EUCC eliminates the obligation for manufacturers to carry out a third-party assessment as *required pursuant to* this Regulation for corresponding requirements.

(83) *The current European standardisation framework, which is based on the New Approach principles set out in Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards and on Regulation (EU) No 1025/2012, represents the framework by default to elaborate standards that provide for a presumption of conformity with the relevant essential cybersecurity requirements set out in this Regulation. European standards should be market-driven, take into account the public interest, as well as the policy objectives clearly stated in the Commission's request to one or more European standardisation organisations to draft harmonised standards, within a set deadline, and be based on consensus. However, in the absence of relevant references to harmonised standards, the Commission should be able to adopt implementing acts establishing common specifications for the essential cybersecurity requirements set out in this Regulation, provided that in doing so it duly respects the role and functions of standardisation organisations, as an exceptional fall back solution to facilitate the manufacturer's obligation to comply with those essential cybersecurity requirements, where the standardisation process is blocked or where there are delays in the establishment of appropriate harmonised standards. If such delay is due to the technical complexity of the standard in question, this should be considered by the Commission before considering whether to establish common specifications.*

- (84) *With a view to establishing, in the most efficient way, common specifications that cover the essential cybersecurity requirements set out in this Regulation, the Commission should involve relevant stakeholders in the process.*
- (85) *‘Reasonable period’ has the meaning, in relation to the publication of a reference to harmonised standards in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012, of a period during which the publication in the Official Journal of the European Union of the reference to the standard, its corrigendum or its amendment is expected and which should not exceed one year after the deadline for drafting a European standard set in accordance with Regulation (EU) No 1025/2012.*
- (86) *In order to facilitate the assessment of conformity with the essential cybersecurity requirements set out in 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 pursuant to this Regulation for the purpose of expressing detailed technical specifications of those requirements.*

(87) *The application of harmonised standards, common specifications or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 providing presumption of conformity in relation to the essential cybersecurity requirements applicable to products with digital elements will facilitate the assessment of conformity by the manufacturers. If the manufacturer chooses not to apply such means for certain requirements, it has to indicate in their technical documentation how the compliance is reached otherwise. Furthermore, the application of harmonised standards, common specifications or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 providing presumption of conformity by manufacturers would facilitate the check of compliance of products with digital elements by market surveillance authorities. Therefore, manufacturers of products with digital elements are encouraged to apply such harmonised standards, common specifications or European cybersecurity certification schemes.*

- (88) 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 cybersecurity requirements *set out in* this Regulation and, where applicable, of the other relevant Union harmonisation legislation by which the product *with digital elements* is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union *legal acts*. 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 legal 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.

- (89) 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 Council²⁸. 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 *set out in* this Regulation.

²⁸ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(90) In order to allow economic operators to demonstrate conformity with the essential cybersecurity requirements **set out** in this Regulation and to allow market surveillance authorities to ensure that products with digital elements made available on the market comply with *those* requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council²⁹ 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 cybersecurity requirements set out in this Regulation **should be** based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole lifecycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product **with digital elements**.

²⁹ Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

(91) **■** Conformity assessment of products with digital elements *that are not listed as important or critical products with digital elements in this Regulation* can be carried out by the manufacturer under its own responsibility following the *internal control* procedure based on Module A of Decision No 768/2008/EC *in accordance with this Regulation. This also applies to cases where a manufacturer chooses not to apply in whole or in part an applicable harmonised standard, common specification or European cybersecurity certification scheme.* The manufacturer *retains* the flexibility to choose a stricter conformity assessment procedure involving a third party. *Under the internal control conformity assessment procedure, the manufacturer ensures and declares on its sole responsibility that the product with digital elements and the processes of the manufacturer meet the applicable essential cybersecurity requirements set out in this Regulation. If an important product with digital elements falls under class I, additional assurance is required to demonstrate conformity with the essential cybersecurity requirements set out in this Regulation. The manufacturer should apply harmonised standards, common specifications or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act if it wants to carry out the conformity assessment under its own responsibility (module A). If the manufacturer does not apply such harmonised standards, common specifications or European cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party (based on modules B and C or module H).* 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 based on modules B *and* C or module H of Decision No 768/2008/EC have been chosen as most appropriate for assessing the compliance of *important* 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 *best* suits its design and production process. Given the even greater cybersecurity risk linked with the use of *important* products *with digital elements that fall under class II ■*, the conformity assessment should always involve a third party, *even where the product complies fully or partly with harmonised standards, common specifications or European cybersecurity certification schemes. Manufacturers of*

important products with digital elements qualifying as free and open-source software should be able to follow the internal control procedure based on Module A, provided that they make the technical documentation available to the public.

(92) 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. Those activities should be considered to be activities amounting to production when applying the relevant conformity assessment modules to verify the compliance of the product with the essential cybersecurity requirements *set out in* this Regulation across the design, development and production phases.

(93) *In relation to microenterprises and small enterprises, in order to ensure proportionality, it is appropriate to alleviate administrative costs without affecting the level of cybersecurity protection of products with digital elements that fall within the scope of this Regulation or the level playing field among manufacturers. It is therefore appropriate for the Commission to establish a simplified technical documentation form targeted at the needs of microenterprises and small enterprises. The simplified technical documentation form adopted by the Commission should cover all the applicable elements related to technical documentation set out in this Regulation and specify how a microenterprise or a small enterprise can provide the requested elements in a concise way, such as the description of the design, development and production of the product with digital elements. In doing so, the form would contribute to alleviating the administrative compliance burden by providing the enterprises concerned with legal certainty about the extent and detail of information to be provided. Microenterprises and small enterprises should be able to choose to provide the applicable elements related to technical documentation in extensive form and not take advantage of the simplified technical form available to them.*

(94) In order to promote and protect innovation, it is important that the interests of manufacturers that are microenterprises or small or medium-sized enterprises, in particular microenterprises and small enterprises, including start-ups, are taken into particular account. To that end, Member States could develop initiatives which are targeted at manufacturers that are microenterprises or small enterprises, including on training, awareness raising, information communication, testing and third-party conformity assessment activities, as well as the establishment of sandboxes. Translation costs related to mandatory documentation, such as the technical documentation and the information and instructions to the user required pursuant to this Regulation, and communication with authorities, may constitute a significant cost for manufacturers, in particular those of a smaller size. Therefore, Member States should be able to consider that one of the languages determined and accepted by them for relevant manufacturers' documentation and for communication with manufacturers is one which is broadly understood by the largest possible number of users.

- (95) *In order to ensure a smooth application of this Regulation, Member States should strive to ensure, before the date of application of this Regulation, that a sufficient number of notified bodies is available to carry out third-party conformity assessments. The Commission should seek to assist Member States and other relevant parties in this endeavour, in order to avoid bottlenecks and hindrances to market entry for manufacturers. Targeted training activities led by Member States, including where appropriate with the support of the Commission, can contribute to the availability of skilled professionals including to support the activities of notified bodies under this Regulation. Furthermore, in light of the costs that third-party conformity assessment may entail, funding initiatives at Union and national level that seek to alleviate such costs for microenterprises and small enterprises should be considered.*
- (96) *In order to ensure proportionality, conformity assessment bodies, when setting the fees for conformity assessment procedures, should take into account the specific interests and needs of microenterprises and small and medium-sized enterprises, including start-ups. In particular, conformity assessment bodies should apply the relevant examination procedure and tests provided for in this Regulation only where appropriate and following a risk-based approach.*

- (97) *The objectives of regulatory sandboxes should be to foster innovation and competitiveness for businesses by establishing controlled testing environments before the placing on the market of products with digital elements. Regulatory sandboxes should contribute to improve legal certainty for all actors that fall within the scope of this Regulation and facilitate and accelerate access to the Union market for products with digital elements, in particular when provided by microenterprises and small enterprises, including start-ups.*
- (98) 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 **comply** with a set of requirements, **in particular** on independence, competence and absence of conflicts of interest.

- (99) 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.
- (100) *Conformity assessment bodies that have been accredited and notified under Union law laying down requirements similar to those laid down in this Regulation, such as a conformity assessment body that has been notified for a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881 or notified under Delegated Regulation (EU) 2022/30, should be newly assessed and notified under this Regulation. However, synergies can be defined by relevant authorities regarding any overlapping requirements in order to prevent an unnecessary financial and administrative burden and to ensure a smooth and timely notification process.*

- (101) 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 to be 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.
- (102) 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 a 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.

- (103) 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.
- (104) 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.

- (105) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.
- (106) Market surveillance is an essential instrument in ensuring the proper and uniform application of Union *law*. It is therefore appropriate to put in place a legal framework within which market surveillance can be carried out in an appropriate manner. The rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 apply to products with digital elements *that fall within the scope of* this Regulation.

(107) In accordance with Regulation (EU) 2019/1020, a market surveillance authority carries out market surveillance in the territory of the Member State that designates it. This Regulation should not prevent Member States from choosing the competent authorities to carry out market surveillance tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States *should be able to* choose to designate any existing or new authority to act as market surveillance authority, including competent authorities *designated or established pursuant to* Article 8 of Directive (EU) 2022/2555, national cybersecurity certification authorities *designated pursuant to* Article 58 of Regulation (EU) 2019/881 *or market surveillance authorities designated for the purposes of Directive 2014/53/EU*. 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 *market* surveillance tasks relating to this Regulation. *Pursuant to* 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.

- (108) 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. 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 *pursuant to* Article 29 of Regulation (EU) 2019/1020 and comprising representatives from each Member State, including a representative of each single liaison office as referred to in Article 10 of *that* Regulation and an optional national expert, the chairs of ADCOs, and representatives from the Commission. The Commission should participate in the meetings of the Union **Product Compliance** Network, its sub-groups and ADCO. It should also assist ADCO by means of an executive secretariat that provides technical and logistic support. *ADCO may also invite independent experts to participate, and liaise with other ADCOs, such as that established under Directive 2014/53/EU.*
- (109) *Market surveillance authorities, through ADCO established under this Regulation, should cooperate closely and should be able to develop guidance documents to facilitate market surveillance activities at national level, such as by developing best practices and indicators to effectively check the compliance of products with digital elements with this Regulation.*

(110) 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 under which interested parties are informed of measures intended to be taken with regard to such products should be *provided for*. 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.

(111) In certain cases, a product with digital elements which complies with this Regulation can 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, to the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities as referred to in **Article 3(1) of 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 **with digital elements** 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 *with digital elements* 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 to be justified, the Commission should also consider whether to adopt proposals to revise the *relevant* Union *law*.

(112) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that *they do not comply* with this Regulation, or for products that *comply* with this Regulation, but that present other important risks, such as risks to the health or safety of persons, *to compliance with obligations under Union or national law intended to protect* fundamental rights or to the *availability, authenticity, integrity or confidentiality of* services *offered using an electronic information system* by essential entities as referred to in *Article 3(1) of* Directive (EU) 2022/2555, the Commission *should be able to* request ENISA to carry out an evaluation. Based on that evaluation, the Commission *should be able to* adopt, *by means of* implementing acts, corrective or restrictive measures at Union level, including *requiring the products with digital elements concerned to be withdrawn* from the market or recalled, within a reasonable period, commensurate with the nature of the risk. The Commission *should be able to* have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the *proper* functioning of the internal market, and only where no effective measures have been taken by *market* surveillance authorities to remedy the situation.

Such exceptional circumstances may be emergency situations where, for example, a non-compliant product *with digital elements* 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 *should be able to* intervene in such emergency situations only for the duration of the exceptional circumstances and if non-compliance with this Regulation or the important risks presented persist.

- (113) *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.

(114) 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 categories *of products with digital elements* are often found to present cybersecurity risks. ***Furthermore, when determining the product categories to be subjected to sweeps, market surveillance authorities should also take into account circumstances relating to non-technical risk factors. To that end, market surveillance authorities should be able to take into account the results of Union level coordinated security risk assessments of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555, including circumstances relating to non-technical risk factors.*** ENISA should submit proposals for categories of products *with digital elements* for which sweeps could be organised to the market surveillance authorities, based, among others, on the notifications of vulnerabilities and incidents it receives.

- (115) ***In light of*** its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, ENISA 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 ***sweeps*** should be organised. In exceptional circumstances, ENISA should be able, at the request of the Commission, 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 proper functioning of the internal market.
- (116) ***This Regulation confers certain tasks upon ENISA which require appropriate resources in terms of both expertise and human resources in order to enable ENISA to carry out those tasks effectively. The Commission will propose the necessary budgetary resources for ENISA’s establishment plan, in accordance with the procedure set out in Article 29 of Regulation (EU) 2019/881, when preparing the draft general budget of the Union. During that process, the Commission will consider ENISA’s overall resources to enable it to fulfil its tasks, including those conferred on ENISA pursuant to this Regulation.***

(117) 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 *on the Functioning of the European Union (TFEU)* should be delegated to the Commission in respect of *updating an annex listing the important products with digital elements*. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential mandating of certification *under a European cybersecurity certification scheme of the critical products with digital elements set out in an annex to this Regulation, as well as for updating the list of critical products with digital elements based on criticality criteria set out in this Regulation, and for specifying the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential cybersecurity requirements or parts thereof as set out in an annex to this Regulation.*

*Power to adopt acts should also be delegated to the Commission to specify the minimum support period for specific product categories where the market surveillance data suggests inadequate support periods, as well as to specify the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications of actively exploited vulnerabilities. Furthermore, power to adopt acts should be delegated to the Commission to establish voluntary security attestation programmes for assessing the conformity of products with digital elements qualifying as free and open-source software with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation, as well as to specify the minimum content of the EU declaration of conformity and to supplement the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the *Interinstitutional* Agreement of 13 April 2016 on Better Law-Making³⁰.*

³⁰ OJ L 123, 12.5.2016, p. 1.

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. ***The power to adopt delegated acts pursuant to this Regulation should be conferred on the Commission for a period of five years from ... [date of entry into force of this Regulation]. The Commission should draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power should be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.***

(118) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to specify the ***technical description of the categories of important products with digital elements set out in an annex to this Regulation, specify the*** format and elements of the SBOM, specify further the **■** format and procedure of the notifications of actively exploited vulnerabilities and ***severe incidents having an impact on the security of products with digital elements submitted by manufacturers, establish common specifications covering technical requirements that provide a means to comply*** with the essential cybersecurity requirements **■** set out in an annex ***to*** this Regulation, **■** lay down technical specifications for ***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 and to increase public awareness about the security of products with digital elements, specify the simplified documentation form targeted at the needs of microenterprises and small enterprises, and*** decide on corrective or restrictive measures at Union level in exceptional circumstances which justify an immediate intervention to preserve the ***proper*** 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 Council³¹.

³¹ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13, ELI: <http://data.europa.eu/eli/reg/2011/182/oj>).

- (119) In order to ensure *trusting* 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.
- (120) 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 law 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 or a small or medium-sized enterprise, including a start-up*, and whether administrative fines have been already applied by *the same or* other market surveillance authorities to the same *economic* operator for a similar infringement.

Such circumstances *could* be either aggravating, in situations where the infringement by the same *economic* operator persists on the territory of Member States *other* than that 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 *infringement* 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. ***Given that administrative fines do not apply to microenterprises or small enterprises for a failure to meet the 24-hour deadline for the early warning notification of actively exploited vulnerabilities or severe incidents having an impact on the security of the product with digital elements, nor to open-source software stewards for any infringement of this Regulation, and subject to the principle that penalties should be effective, proportionate and dissuasive, Member States should not impose other kinds of penalties with pecuniary character on those entities.***

(121) Where administrative fines are imposed on a person that *is* 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.

(122) *Member States should examine, taking into account national circumstances, the possibility of using the revenues from the penalties as provided for in this Regulation or their financial equivalent to support cybersecurity policies and increase the level of cybersecurity in the Union by, inter alia, increasing the number of qualified cybersecurity professionals, strengthening capacity building for microenterprises and small and medium-sized enterprises and improving public awareness of cyber threats.*

(123) In its relationships with third countries, the *Union* 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. Those 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 with several third countries. Those MRAs are concluded in a number of specific sectors, which might vary from one third 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 *can* be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU. Cooperation with partner third 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 *Union*.

(124) Consumers should be entitled to enforce their rights in relation to the obligations imposed on economic operators under this Regulation through representative actions pursuant to Directive (EU) 2020/1828 of the European Parliament and of the Council³². For that purpose, this Regulation should provide that Directive (EU) 2020/1828 is applicable to the representative actions concerning infringements of this Regulation that harm or can harm the collective interests of consumers. Annex I to that Directive should therefore be amended accordingly. It is for the Member States to ensure that those amendments are reflected in the transposition measures adopted pursuant to that Directive, although the adoption of national transposition measures in that regard is not a condition for the applicability of that Directive to those representative actions. The applicability of that Directive to the representative actions brought with regard to infringements of provisions of this Regulation by economic operators that harm or could harm the collective interests of consumers should start from ... [36 months from the date of entry into force of this Regulation].

³² **Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).**

- (125) The Commission should periodically *evaluate and* review this Regulation, in consultation with *relevant stakeholders*, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions. *This Regulation will facilitate the compliance with supply chain security obligations of entities that fall within the scope of Regulation (EU) 2022/2554 and Directive (EU) 2022/2555 that use products with digital elements. The Commission should evaluate, as part of that periodic review, the combined effects of the Union cybersecurity framework.*
- (126) Economic operators should be provided with sufficient time to adapt to the requirements set out in this Regulation. This Regulation should apply from ... [36 months *from the date of entry into force of this Regulation*], with exception of the reporting obligations concerning actively exploited vulnerabilities and *severe* incidents *having an impact on the security of products with digital elements*, which should apply from ... [21 months *from the date of entry into force of this Regulation*] and of the provisions on notification of conformity assessment bodies, which should apply from ... [18 months] from the *date of entry into force of this Regulation*].

(127) *It is important to provide support to microenterprises and small and medium-sized enterprises, including start-ups, in the implementation of this Regulation and to minimise the risks to the implementation resulting from lack of knowledge and expertise in the market, as well as in order to facilitate compliance of manufacturers with their obligations laid down in this Regulation. The Digital Europe Programme and other relevant Union programmes provide financial and technical support that enable those enterprises to contribute to the growth of the Union economy and to the strengthening of the common level of cybersecurity in the Union. The European Cybersecurity Competence Centre and National Coordination Centres as well as European Digital Innovation Hubs established by the Commission and the Member States at Union or national level could also support companies and public sector organisations and could contribute to the implementation of this Regulation. Within their respective missions and fields of competence, they could provide technical and scientific support to microenterprises and small and medium sized enterprises, such as for testing activities and third-party conformity assessments. They could also foster the deployment of tools to facilitate the implementation of this Regulation.*

(128) *Furthermore, Member States should consider taking complementary action aiming to provide guidance and support for microenterprises and small and medium-sized enterprises, such as the establishment of regulatory sandboxes and dedicated channels for communication. In order to strengthen the level of cybersecurity in the Union, Member States may also consider providing support to develop capacity and skills related to cybersecurity of products with digital elements, improving the cyber resilience of economic operators, in particular of microenterprises and small and medium-sized enterprises, and fostering public awareness about the cybersecurity of products with digital elements.*

- (129) 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.
- (130) 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 Council³³ and delivered *an* opinion on **9 November 2022**³⁴,

HAVE ADOPTED THIS REGULATION:

³³ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

³⁴ ***OJ C 452, 29.11.2022, p. 23.***

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 cybersecurity requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;
- (c) essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the ***time the products are expected to be in use***, and obligations for economic operators in relation to those processes;
- (d) rules on market surveillance, ***including monitoring***, and enforcement of the rules and requirements ***referred to in this Article***.

Article 2

Scope

1. This Regulation applies to products with digital elements ***made available on the market, the intended purpose*** or reasonably foreseeable use ***of which*** includes a direct or indirect logical or physical data connection to a device or network.
2. This Regulation does not apply to products with digital elements to which the following Union ***legal*** acts apply:
 - (a) Regulation (EU) 2017/745;
 - (b) Regulation (EU) 2017/746;
 - (c) Regulation (EU) 2019/2144.
3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.
4. ***This Regulation does not apply to equipment that falls within the scope of Directive 2014/90/EU of the European Parliament and of the Council³⁵.***

³⁵ ***Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).***

5. 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 cybersecurity requirements set out in Annex I may be limited or excluded where:
- (a) such limitation or exclusion is consistent with the overall regulatory framework *that* applies to those products; and
 - (b) the sectoral rules achieve the same *or a higher* level of protection as that provided for by this Regulation.

The Commission is empowered to adopt delegated acts in accordance with Article **61** to *supplement* this Regulation *by* specifying whether such limitation or exclusion is necessary, the products and rules *concerned*, as well as the scope of the limitation, if relevant.

6. *This Regulation does not apply to spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace.*

7. This Regulation does not apply to products with digital elements developed *or modified* exclusively for national security *or defence* purposes or to products specifically designed to process classified information.
8. *The obligations laid down in this Regulation shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.*

Article 3 Definitions

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

- (1) 'product with digital elements' means a software or hardware product and its remote data processing solutions, including software or hardware components *being* placed on the market separately;
- (2) 'remote data processing' means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

- (3) *‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;*
- (4) ‘software’ means the part of an electronic information system which consists of computer code;
- (5) ‘hardware’ means a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data;
- (6) ‘component’ means software or hardware intended for integration into an electronic information system;
- (7) ‘electronic information system’ means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;
- (8) ‘logical connection’ means a virtual representation of a data connection implemented through a software interface;
- (9) ‘physical connection’ means a connection between electronic information systems or components implemented using physical means, including through electrical, *optical* or mechanical interfaces, wires or radio waves;

(10) ‘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;



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



(12) ‘economic operator’ means the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations *in relation to the manufacture of products with digital elements or to the making available of products with digital elements on the market in accordance with* this Regulation;

(13) ‘manufacturer’ means a 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 *its* name or trademark, whether for payment, *monetisation* or free of charge;

- (14) *‘open-source software steward’ means a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products;*
- (15) ‘authorised representative’ means a natural or legal person established within the Union who has received a written mandate from a manufacturer to act on *its* behalf in relation to specified tasks;
- (16) ‘importer’ means a 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;
- (17) ‘distributor’ means a 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;

- (18) *‘consumer’ means a natural person who acts for purposes which are outside that person’s trade, business, craft or profession;*
- (19) *‘microenterprises’, ‘small enterprises’ and ‘medium-sized enterprises’ mean, respectively, microenterprises, small enterprises and medium-sized enterprises as defined in the Annex to Commission Recommendation 2003/361/EC;*
- (20) *‘support period’ means the period during which a manufacturer is required to ensure that vulnerabilities of a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I;*
- (21) ‘placing on the market’ means the first making available of a product with digital elements on the Union market;
- (22) ‘making available on the market’ means *the* 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;

- (23) ‘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;
- (24) ‘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;
- (25) ‘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;
- (26) ‘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;

- (27) ‘conformity assessment’ means the process of verifying whether the essential cybersecurity requirements set out in Annex I have been fulfilled;
- (28) ‘conformity assessment body’ means a *conformity assessment* body *as* defined in Article 2, *point (13)*, of Regulation (EC) No 765/2008;
- (29) ‘notified body’ means a conformity assessment body designated in accordance with Article 43 and other relevant Union harmonisation legislation;
- (30) ‘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 cybersecurity requirements set out in Part I of Annex I or *which* results in a modification to the intended *purpose* for which the product with digital elements has been assessed;
- (31) ‘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 cybersecurity requirements set out in Annex I and other applicable Union harmonisation legislation providing for its affixing;

- (32) ***‘Union harmonisation legislation’ means Union legislation listed in Annex I to Regulation (EU) 2019/1020 and any other Union legislation harmonising the conditions for the marketing of products to which that Regulation applies;***
- (33) ***‘market surveillance authority’ means a market surveillance authority as defined in Article 3, point (4), of Regulation (EU) 2019/1020;***
- (34) ***‘international standard’ means an international standard as defined in Article 2, point (1)(a), of Regulation (EU) No 1025/2012;***
- (35) ***‘European standard’ means a European standard as defined in Article 2, point (1)(b), of Regulation (EU) No 1025/2012;***
- (36) ***‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012;***
- (37) ***‘cybersecurity risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;***

- (38) ‘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;
- (39) ‘software bill of materials’ means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;
- (40) ‘vulnerability’ means a *weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat*;
- (41) ‘*exploitable vulnerability*’ means a *vulnerability that has the potential to be effectively used by an adversary under practical operational conditions*;
- (42) ‘actively exploited vulnerability’ means a vulnerability for which there is reliable evidence that *a* malicious ■ actor *has exploited it in* a system without permission of the system owner;
- (43) ‘*incident*’ means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

- (44) *‘incident having an impact on the security of the product with digital elements’ means an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions;*
- (45) *‘near miss’ means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;*
- (46) *‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;*
- (47) *‘personal data’ means **personal** data as defined in Article 4, point (1), of Regulation (EU) 2016/679;*
- (48) *‘free and open-source software’ means software the source code of which is openly shared and which is made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable;*
- (49) *‘recall’ means recall as defined in Article 3, point (22), of Regulation (EU) 2019/1020;*

(50) *'withdrawal' means withdrawal as defined in Article 3, point (23), of Regulation (EU) 2019/1020;*

(51) *'CSIRT designated as coordinator' means a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555.*

Article 4

Free movement

1. Member States shall not impede, for the matters covered by this Regulation, the making available on the market of products with digital elements which comply with this Regulation.
2. At trade fairs, exhibitions, demonstrations or similar events, Member States shall not prevent the presentation *or* use of a product with digital elements which does not comply with this Regulation, ***including its prototypes, provided that the product is presented with a visible sign clearly indicating that it does not comply with this Regulation and is not to be made available on the market until it does so.***

3. Member States shall not prevent the making available *on the market* of unfinished software which does not comply with this Regulation, provided that the software is made available only for a limited period required for testing purposes with a visible sign clearly indicating that it does not comply with this Regulation and will not be available on the market for purposes other than testing.
4. *Paragraph 3 does not apply to safety components as referred to in Union harmonisation legislation other than this Regulation.*

Article 5

Procurement or use of products with digital elements

1. *This Regulation shall not prevent Member States from subjecting products with digital elements to additional cybersecurity requirements for the procurement or use of those products for specific purposes, including where those products are procured or used for national security or defence purposes, provided that such requirements are consistent with Member States' obligations laid down in Union law and that they are necessary and proportionate for the achievement of those purposes.*

2. ***Without prejudice to Directives 2014/24/EU and 2014/25/EU, where products with digital elements that fall within the scope of this Regulation are procured, Member States shall ensure that compliance with the essential cybersecurity requirements set out in Annex I to this Regulation, including the manufacturers' ability to handle vulnerabilities effectively, are taken into consideration in the procurement process.***

Article 6

Requirements for products with digital elements

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

- (a) they meet the essential cybersecurity requirements set out in Part I of Annex I, ***provided*** that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, ***the necessary security updates have been installed***; and
- (b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.

Article 7

Important products with digital elements

1. Products with digital elements ***which have the core functionality of a product category set out in Annex III shall be considered to be important products with digital elements and shall be subject to the conformity assessment procedures referred to in Article 32(2) and (3). The integration of a product with digital elements which has the core functionality of a product category set out in Annex III shall not in itself render the product in which it is integrated subject to the conformity assessment procedures referred to in Article 32(2) and (3).***

2. ***The categories of products with digital elements referred to in paragraph 1 of this Article, divided into classes I and II as set out in Annex III, meet at least one of the following criteria:***
 - (a) ***the product with digital elements primarily performs functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;***

(b) the product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.

3. The Commission is empowered to adopt delegated acts in accordance with Article 61 to amend Annex III by including in the list **a new category within each class of the** categories of **■** products with digital elements **and specifying its definition, moving a category of products from one class to the other** or withdrawing an existing **category** from that list. When assessing the need to amend the list **set out** in Annex III, the Commission shall take into account the **cybersecurity-related functionalities or the function and the level of cybersecurity risk posed by the products with digital elements as set out by the criteria referred to in paragraph 2 of this Article.**

*The delegated acts referred to in the first subparagraph of this paragraph shall, where appropriate, provide for a minimum transitional period of 12 months, in particular where a new category of **important** products with digital elements is added to class I or II or is moved from class I to II as set out in Annex III, before the relevant conformity assessment procedures as referred to in Article 32(2) and (3) start applying, unless a shorter transitional period is justified on imperative grounds of urgency.*

4. *By ... [12 months from the date of entry into force of this Regulation], the Commission shall adopt an implementing act specifying the **technical description** of the **categories of products with digital elements** under classes I and II as set out in Annex III **and the technical description of the categories of products with digital elements as set out in Annex IV**. That implementing act shall be adopted **in accordance with the examination procedure referred to in Article 62(2)**.*

Article 8

Critical products with digital elements

- 1. The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation to determine which products with digital elements that have the core functionality of a product category that is set out in Annex IV to this Regulation are to be required to obtain a European cybersecurity certificate at assurance level at least ‘substantial’ under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881, to demonstrate conformity with the essential cybersecurity requirements set out in Annex I to this Regulation or parts thereof, provided that a European cybersecurity certification scheme covering those categories of products with digital elements has been adopted pursuant to Regulation (EU) 2019/881 and is available to manufacturers. Those delegated acts shall specify the required assurance level that shall be proportionate to the level of cybersecurity risk associated with the products with digital elements and shall take account of their intended purpose, including the critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555.*

Before adopting such delegated acts, the Commission shall carry out an assessment of the potential market impact of the envisaged measures and shall carry out consultations with relevant stakeholders, including the European Cybersecurity Certification Group established under Regulation (EU) 2019/881. The assessment shall take into account the readiness and the capacity level of the Member States for the implementation of the relevant European cybersecurity certification scheme. Where no delegated acts as referred to in the first subparagraph of this paragraph have been adopted, products with digital elements which have the core functionality of a product category as set out in Annex IV shall be subject to the conformity assessment procedures referred to in Article 32(3).

The delegated acts referred to in the first subparagraph shall provide for a minimum transitional period of six months, unless a shorter transitional period is justified for imperative reasons of urgency.

2. The Commission is empowered to adopt delegated acts in accordance with Article 61 to *amend Annex IV by adding or withdrawing* categories of critical products with digital elements. *When determining such categories of critical products with digital elements and the required assurance level, in accordance with paragraph 1 of this Article*, the Commission shall take into account the *criteria referred to in Article 7(2) and ensure that the categories of products with digital elements meet at least one of the following criteria*:

- (a) *there is a critical dependency of essential entities* as referred to in Article 3 of Directive (EU) 2022/2555 on the category of products with digital elements;
- (b) *incidents and exploited vulnerabilities concerning the category* of products with digital elements *could lead to serious disruptions of critical supply chains across the internal market*.

Before adopting such delegated acts, the Commission shall carry out an assessment of the type referred to in paragraph 1.

The delegated acts referred to in the first subparagraph shall provide for a minimum transitional period of six months, unless a shorter transitional period is justified for imperative reasons of urgency.

Article 9

Stakeholder consultation

- 1.** *When preparing measures for the implementation of this Regulation, the Commission shall consult and take into account the views of relevant stakeholders, such as relevant Member State authorities, private sector undertakings, including microenterprises and small and medium-sized enterprises, the open-source software community, consumer associations, academia, and relevant Union agencies and bodies as well as expert groups established at Union level. In particular, the Commission shall, in a structured manner, where appropriate, consult and seek the views of those stakeholders when:*
 - (a)** *preparing the guidance referred to in Article 26;*
 - (b)** *preparing the technical descriptions of the product categories set out in Annex III in accordance with Article 7(4), assessing the need for potential updates of the list of product categories in accordance with Article 7(3) and Article 8(2), or carrying out the assessment of the potential market impact referred to in Article 8(1), without prejudice to Article 61;*

(c) undertaking preparatory work for the evaluation and review of this Regulation.

2. The Commission shall organise regular consultation and information sessions, at least once a year, to gather the views of the stakeholders referred to in paragraph 1 on the implementation of this Regulation.

Article 10

Enhancing skills in a cyber resilient digital environment

For the purposes of this Regulation and in order to respond to the needs of professionals in support of the implementation of this Regulation, Member States with, where appropriate, the support of the Commission, the European Cybersecurity Competence Centre and ENISA, while fully respecting the responsibility of the Member States in the education field, shall promote measures and strategies aiming to:

(a) develop cybersecurity skills and create organisational and technological tools to ensure sufficient availability of skilled professionals in order to support the activities of the market surveillance authorities and conformity assessment bodies;

- (b) *increase collaboration between the private sector, economic operators, including via re-skilling or up-skilling for manufacturers' employees, consumers, training providers as well public administrations, thereby expanding the options for young people to access jobs in the cybersecurity sector.*

Article 11

General product safety

By way of 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 *that* Regulation ■ shall apply to ■ products with *digital elements with* respect to *aspects and risks or categories of risks that are* not covered by this Regulation *where those products are not subject to specific safety requirements laid down in other 'Union harmonisation legislation' as defined in Article 3, point (27), of Regulation (EU) 2023/988.*

Article 12

High-risk AI systems

1. ***Without prejudice to the requirements relating to accuracy and robustness set out in Article 15 of Regulation (EU) 2024/1689, products with digital elements which fall within the scope of this Regulation and which are classified as high-risk AI systems pursuant to Article 6 of that Regulation shall be deemed to comply with the cybersecurity requirements set out in Article 15 of that Regulation where:***
 - (a) those products fulfil the essential cybersecurity requirements set out in Part I of Annex I;***
 - (b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I; and***
 - (c) the achievement of the level of cybersecurity protection required under Article 15 of Regulation (EU) 2024/1689 is demonstrated in the EU declaration of conformity issued under this Regulation.***

2. For the products *with digital elements* and cybersecurity requirements referred to in paragraph 1 *of this Article*, the relevant conformity assessment procedure *provided for in* Article 43 of Regulation (EU) 2024/1689 shall apply. For the purposes of that assessment, notified bodies which are *competent* to control the conformity of the high-risk AI systems under Regulation (EU) 2024/1689 shall also *be competent* to control the conformity of high-risk AI systems *which 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 39 of this Regulation *has* been assessed in the context of the notification procedure under Regulation (EU) 2024/1689.

3. By *way of* derogation from paragraph 2 of this Article, **important** products with digital elements as listed in Annex III *to* this Regulation, which **are subject to** the conformity assessment procedures referred to in Article 32(2), **points** (a) **and** (b), and Article 32(3) **of this Regulation and critical products with digital elements as listed in Annex IV to this Regulation which are required to obtain a European cybersecurity certificate pursuant to Article 8(1) of this Regulation or, absent that, which are subject to the conformity assessment procedures referred to in Article 32(3) of this Regulation**, and which are classified as high-risk AI systems **pursuant** to Article 6 of **Regulation (EU) 2024/1689**, and to which the conformity assessment procedure based on internal control as referred to in Annex VI to Regulation **(EU) 2024/1689** applies, shall be subject to the conformity assessment procedures **provided for in** this Regulation in so far as the essential cybersecurity requirements set out in this Regulation are concerned.
4. **Manufacturers of products with digital elements referred to in paragraph 1 of this Article may participate in the AI regulatory sandboxes referred to in Article 57 of Regulation (EU) 2024/1689.**

█

CHAPTER II
OBLIGATIONS OF ECONOMIC OPERATORS *AND PROVISIONS IN RELATION TO FREE
AND OPEN-SOURCE SOFTWARE*

Article 13
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 cybersecurity requirements set out in Part I of Annex I.
2. For the purpose of complying with 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 incidents and minimising their impact, including in relation to the health and safety of users.

3. *The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.*

4. When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment *referred to in paragraph 3 of this Article* in the technical documentation *required pursuant to* Article 31 and Annex VII. For products with digital elements as referred to in Article 12, *which* are also subject to other Union *legal* acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union *legal* acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that *technical* documentation.

5. For the purpose of complying with paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties *so* that *those* components do not compromise the *cybersecurity 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.*

6. *Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex I. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.*
7. The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities *of which they become* aware and any relevant information provided by third parties, and *shall*, where applicable, update the *cybersecurity* risk assessment of the products.

8. ***Manufacturers shall ensure***, when placing a product with digital elements on the market, and for the ***support period***, ***that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I.***

Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements. When determining the support period, manufacturers may also take into account the support periods of products with digital elements offering a similar functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components that provide core functions and are sourced from third parties as well as relevant guidance provided by the dedicated administrative cooperation group (ADCO) established pursuant to Article 52(15) and the Commission. The matters to be taken into account in order to determine the support period shall be considered in a manner that ensures proportionality.

Without prejudice to the second subparagraph, the support period shall be at least five years. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.

Taking into account ADCO recommendations as referred to in Article 52(16), the Commission may adopt delegated acts in accordance with Article 61 to supplement this Regulation by specifying the minimum support period for specific product categories where the market surveillance data suggests inadequate support periods.

Manufacturers shall include the information that was taken into account to determine the support period of a product with digital elements in the technical documentation as set out in Annex VII.

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

9. *Manufacturers shall ensure that each security update, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer.*
10. *Where a manufacturer has placed subsequent substantially modified versions of a software product on the market, that manufacturer may ensure compliance with the essential cybersecurity requirement set out in Part II, point (2), of Annex I only for the version that it has last placed on the market, provided that the users of the versions that were previously placed on the market have access to the version last placed on the market free of charge and do not incur additional costs to adjust the hardware and software environment in which they use the original version of that product.*
11. *Manufacturers may maintain public software archives enhancing user access to historical versions. In those cases, users shall be clearly informed in an easily accessible manner about risks associated with using unsupported software.*

12. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 31.

They shall carry out the chosen conformity assessment procedures as referred to in Article 32 or have them carried out.

Where compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 28 and affix the CE marking in accordance with Article 30.

13. Manufacturers shall keep the technical documentation and the EU declaration of conformity ■ at the disposal of the market surveillance authorities for *at least 10* years *after the product with digital elements has been placed on the market or for the support period, whichever is longer.*

14. 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 *with this Regulation*. Manufacturers shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or common specifications as referred to in Article 27 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.
15. *Manufacturers shall ensure that their products with digital elements bear a type, batch or serial number or other element allowing their identification, or, where that is not possible, that that information is provided on their packaging or in a document accompanying the product with digital elements.*

16. *Manufacturers shall indicate the name, registered trade name or registered trademark of the manufacturer, and the postal address, email address or other digital contact details, as well as, where applicable, the website where the manufacturer can be contacted, on the product with digital elements, on its packaging or in a document accompanying the product with digital elements. That information shall also be included in the information and instructions to the user set out in Annex II. The contact details shall be in a language which can be easily understood by users and market surveillance authorities.*

17. *For the purposes of this Regulation, manufacturers shall designate a single point of contact to enable users to communicate directly and rapidly with them, including in order to facilitate reporting on vulnerabilities of the product with digital elements.*

Manufacturers shall ensure that the single point of contact is easily identifiable by the users. They shall also include the single point of contact in the information and instructions to the user set out in Annex II.

The single point of contact shall allow users to choose their preferred means of communication and shall not limit such means to automated tools.

18. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions *to the user* set out in Annex II, in *paper or* electronic form. Such information and instructions shall be *provided* in a language which can be easily understood by users *and market surveillance authorities*. They shall be clear, understandable, intelligible and legible. They shall allow for the secure installation, operation and use of products with digital elements. ***Manufacturers shall keep the information and instructions to the user set out in Annex II at the disposal of users and market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. Where such information and instructions are provided online, manufacturers shall ensure that they are accessible, user-friendly and available online for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.***

19. Manufacturers shall ensure that the end date of the support period referred to in paragraph 8, including at least the month and the year, is clearly and understandably specified at the time of purchase in an easily accessible manner and, where applicable, on the product with digital elements, its packaging or by digital means.

Where technically feasible in light of the nature of the product with digital elements, manufacturers shall display a notification to users informing them that their product with digital elements has reached the end of its support period.

20. Manufacturers shall either provide a copy of the EU declaration of conformity or a simplified EU declaration of conformity with the product with digital elements. Where a simplified EU declaration of conformity is provided, it shall contain the exact internet address at which the full EU declaration of conformity can be accessed.

21. From the placing on the market and for *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 cybersecurity 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.
22. Manufacturers shall, *upon* a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by *that authority*, 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 cybersecurity requirements set out in Annex I. *Manufacturers* 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.

23. A manufacturer that ceases its operations and, as a result, is not able to comply with this Regulation shall inform, before the *cessation* of operations takes effect, the relevant market surveillance authorities as well as, by any means available and to the extent possible, the users of the *relevant* products with digital elements placed on the market, *of the impending cessation of operations*.
24. The Commission may, by means of *implementing acts taking into account European or international standards and best practices*, specify the format and elements of the software bill of materials *referred to* in *Part II*, point (1), of Annex I. Those *implementing acts* shall be adopted in accordance with the examination procedure referred to in Article 62(2).

25. *In order to assess the dependence of Member States and of the Union as a whole on software components and in particular on components qualifying as free and open-source software, ADCO may decide to conduct a Union wide dependency assessment for specific categories of products with digital elements. For that purpose, market surveillance authorities may request manufacturers of such categories of products with digital elements to provide the relevant software bills of materials as referred to in Part II, point (1), of Annex I. On the basis of such information, the market surveillance authorities may provide ADCO with anonymised and aggregated information about software dependencies. ADCO shall submit a report on the results of the dependency assessment to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555.*

Article 14

Reporting obligations of manufacturers

1. *A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.*

2. *For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:*

- (a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;*
- (b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;*

- (c) *unless the relevant information has already been provided, a final report, no later than 14 days after 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 malicious 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.*

3. *A manufacturer shall ■ notify ■ any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.*

4. *For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:*
- (a) *an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;*
 - (b) *unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;*

(c) unless the relevant information has already been provided, 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.

5. For the purposes of paragraph 3, an incident having an impact on the security of the product with digital elements shall be considered to be severe where:

(a) it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or

(b) it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

6. *Where necessary, the CSIRT designated as coordinator initially receiving the notification may request manufacturers to provide an intermediate report on relevant status updates about the actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements.*

7. *The notifications referred to in paragraphs 1 and 3 of this Article shall be submitted via the single reporting platform referred to in Article 16 using one of the electronic notification end-points referred to in Article 16(1). The notification shall be submitted using the electronic notification end-point of the CSIRT designated as coordinator of the Member State where the manufacturers have their main establishment in the Union and shall be simultaneously accessible to ENISA.*

For the purposes of this Regulation, a manufacturer shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the manufacturer concerned has the establishment with the highest number of employees in the Union.

Where a manufacturer has no main establishment in the Union, it shall submit the notifications referred to in paragraphs 1 and 3 using the electronic notification end-point of the CSIRT designated as coordinator in the Member State determined pursuant to the following order and based on the information available to the manufacturer:

- (a) the Member State in which the authorised representative acting on behalf of the manufacturer for the highest number of products with digital elements of that manufacturer is established;*
- (b) the Member State in which the importer placing on the market the highest number of products with digital elements of that manufacturer is established;*
- (c) the Member State in which the distributor making available on the market the highest number of products with digital elements of that manufacturer is established;*
- (d) the Member State in which the highest number of users of products with digital elements of that manufacturer are located.*

In relation to the third subparagraph, point (d), a manufacturer may submit notifications related to any subsequent actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements to the same CSIRT designated as coordinator to which it first reported.

8. **■** After becoming aware *of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users*, of that vulnerability or incident and, where necessary, of any *risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.*

9. ***By ... [12 months from the date of entry into force of this Regulation], the Commission shall adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications as referred to in Article 16(2) of this Regulation. The Commission shall cooperate with the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555 and ENISA in preparing the draft delegated acts.***
10. The Commission may, by means of implementing acts, specify further the format and ***procedures*** of the notifications ***referred to in this Article as well as in Articles 15 and 16.*** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). ***The Commission shall cooperate with the CSIRTs network and ENISA in preparing those draft implementing acts.***

█

Article 15

Voluntary reporting

- 1. Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA.*
- 2. Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.*
- 3. The CSIRT designated as coordinator or ENISA shall process the notifications referred to in paragraphs 1 and 2 of this Article in accordance with the procedure laid down in Article 16.*

The CSIRT designated as coordinator may prioritise the processing of mandatory notifications over voluntary notifications.

4. *Where a natural or legal person other than the manufacturer notifies an actively exploited vulnerability or a severe incident having an impact on the security of a product with digital elements in accordance with paragraph 1 or 2, the CSIRT designated as coordinator shall without undue delay inform the manufacturer.*

5. *The CSIRTs designated as coordinators as well as ENISA shall ensure the confidentiality and appropriate protection of the information provided by a notifying natural or legal person. 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 a notifying natural or legal person to which it would not have been subject had it not submitted the notification.*

Article 16

Establishment of a single reporting platform

- 1. For the purposes of the notifications referred to in Article 14(1) and (3) and Article 15(1) and (2) and in order to simplify the reporting obligations of manufacturers, a single reporting platform shall be established by ENISA. The day-to-day operations of that single reporting platform shall be managed and maintained by ENISA. The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification end-points.*
- 2. After receiving a notification, the CSIRT designated as coordinator initially receiving the notification shall, without delay, disseminate the notification via the single reporting platform to the CSIRTs designated as coordinators on the territory of which the manufacturer has indicated that the product with digital elements has been made available.*

In exceptional circumstances and, in particular, upon request by the manufacturer and in light of the level of sensitivity of the notified information as indicated by the manufacturer under Article 14(2), point (a), of this Regulation, the dissemination of the notification may be delayed based on justified cybersecurity-related grounds for a period of time that is strictly necessary, including where a vulnerability is subject to a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555. Where a CSIRT decides to withhold a notification, it shall immediately inform ENISA about the decision and provide both a justification for withholding the notification as well as an indication of when it will disseminate the notification in accordance with the dissemination procedure laid down in this paragraph. ENISA may support the CSIRT on the application of cybersecurity-related grounds in relation to delaying the dissemination of the notification.

In particularly exceptional circumstances, where the manufacturer indicates in the notification referred to in Article 14(2), point (b):

- (a) that the notified vulnerability has been actively exploited by a malicious actor and, according to the information available, it has been exploited in no other Member State than the one of the CSIRT designated as coordinator to which the manufacturer has notified the vulnerability;*
- (b) that any immediate further dissemination of the notified vulnerability would likely result in the supply of information the disclosure of which would be contrary to the essential interests of that Member State; or*
- (c) that the notified vulnerability poses an imminent high cybersecurity risk stemming from the further dissemination;*

only the information that a notification was made by the manufacturer, the general information about the product, the information on the general nature of the exploit and the information that security related grounds were raised are to be made available simultaneously to ENISA until the full notification is disseminated to the CSIRTs concerned and ENISA. Where, based on that information, ENISA considers that there is a systemic risk affecting security in the internal market, it shall recommend to the recipient CSIRT that it disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.

3. *After receiving a notification of an actively exploited vulnerability in a product with digital elements or of a severe incident having an impact on the security of a product with digital elements, the CSIRTs designated as coordinators shall provide the market surveillance authorities of their respective Member States with the notified information necessary for the market surveillance authorities to fulfil their obligations under this Regulation.*

4. *ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single reporting platform and the information submitted or disseminated via the single reporting platform. It shall notify without undue delay any security incident affecting the single reporting platform to the CSIRTs network as well as to the Commission.*

5. *ENISA, in cooperation with the CSIRTs network, shall provide and implement specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single reporting platform referred to in paragraph 1, including at least the security arrangements related to the establishment, operation and maintenance of the single reporting platform, as well as the electronic notification end-points set up by the CSIRTs designated as coordinators at national level and ENISA at Union level, including procedural aspects to ensure that, where a notified vulnerability has no corrective or mitigating measures available, information about that vulnerability is shared in line with strict security protocols and on a need-to-know basis.*

6. *Where a CSIRT designated as coordinator has been made aware of an actively exploited vulnerability as part of a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555, the CSIRT designated as coordinator initially receiving the notification may delay the dissemination of the relevant notification via the single reporting platform based on justified cybersecurity-related grounds for a period that is no longer than is strictly necessary and until consent for disclosure by the involved coordinated vulnerability disclosure parties is given. That requirement shall not prevent manufacturers from notifying such a vulnerability on a voluntary basis in accordance with the procedure laid down in this Article.*

Article 17

Other provisions related to reporting

- 1. ENISA may submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established under Article 16 of Directive (EU) 2022/2555 information notified pursuant to Article 14(1) and (3) and Article 15(1) and (2) of this Regulation if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level. For the purpose of determining such relevance, ENISA may consider technical analyses performed by the CSIRTs network, where available.*
- 2. Where public awareness is necessary to prevent or mitigate a severe incident having an impact on the security of the product with digital elements or to handle an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the CSIRT designated as coordinator of the relevant Member State may, after consulting the manufacturer concerned and, where appropriate, in cooperation with ENISA, inform the public about the incident or require the manufacturer to do so.*

3. *ENISA, on the basis of the notifications received pursuant to Article 14(1) and (3) and Article 15(1) and (2) of this Regulation, shall prepare, every 24 months, a technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555. The first such report shall be submitted within 24 months of the date of application of the obligations laid down in Article 14(1) and (3) of this Regulation. 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.*
4. *The mere act of notification in accordance with Article 14(1) and (3) or Article 15(1) and (2) shall not subject the notifying natural or legal person to increased liability.*

5. *After a security update or another form of corrective or mitigating measure is available, ENISA shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified pursuant to Article 14(1) or Article 15(1) of this Regulation to the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555.*
6. *The CSIRTs designated as coordinators shall provide helpdesk support in relation to the reporting obligations pursuant to Article 14 to manufacturers and in particular manufacturers that qualify as microenterprises or as small or medium-sized enterprises.*

Article 18

Authorised representatives

1. A manufacturer may, by a written mandate, ***appoint an authorised representative.***
2. The obligations laid down in Article 13(1) to (11), Article 13(12), first ***subparagraph,*** and Article 13(14) shall not form part of the authorised representative's mandate.

3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. ***The authorised representative 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 28 and the technical documentation referred to in Article 31 at the disposal of the market surveillance authorities for ***at least 10*** years after the product with digital elements has been placed on the market ***or for the support period, whichever is longer***;
 - (b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;
 - (c) cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.

Article 19
Obligations of importers

1. Importers shall place on the market **only** products with digital elements that comply with the essential cybersecurity requirements set out in Part I of Annex I and where the processes put in place by the manufacturer **comply** with the essential cybersecurity requirements set out in Part II of Annex I.
2. Before placing a product with digital elements on the market, importers shall ensure that:
 - (a) the appropriate conformity assessment procedures as referred to in Article 32 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 30 and is accompanied by the ***EU declaration of conformity referred to in Article 13(20) and the information and instructions to the user*** as set out in Annex II ***in a language which can be easily understood by users and market surveillance authorities***;

(d) the manufacturer has complied with the requirements set out in Article 13(15), (16) and (19).

For the purposes of this paragraph, importers shall be able to provide the necessary documents proving the fulfilment of the requirements set out in this Article.

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 ***this Regulation***, 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 ***this Regulation***. 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.

Where an importer has reason to believe that a product with digital elements may present a significant cybersecurity risk in light of non-technical risk factors, the importer shall inform the market surveillance authorities to that effect. Upon receipt of such information, the market surveillance authorities shall follow the procedures referred to in Article 54(2).

4. Importers shall indicate their name, registered trade name or registered trademark, the postal address, *email address or other digital contact as well as, where applicable, 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 who know or have reason to believe that a product with digital elements which they have placed on the market *is* not in conformity with *this Regulation* shall immediately take the corrective measures necessary to *ensure that the* product with digital elements *is brought* into conformity *with this Regulation*, or to withdraw or recall the product, if appropriate.

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 *have* made the product with digital elements available on the market to that effect, giving details, in particular, of non-compliance and of any corrective measures taken.

6. Importers shall, for *at least* 10 years after the product with digital elements has been placed on the market *or for the support period, whichever is longer*, 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.

7. 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 cybersecurity requirements set out in *Part I* of Annex I as well as of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II 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.

8. Where the importer of a product with digital elements becomes aware that the manufacturer of that product has 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 20

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 *set out in* 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 in Article *13(15), (16)*, (18), (19) *and* (20) and Article 19(4), *and have provided all necessary 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 cybersecurity 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 *with this Regulation*. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform, *without undue delay*, 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 *this Regulation* shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity, or to withdraw or recall the product, if appropriate, are taken.

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-*compliance* and of any corrective measures taken.

5. Distributors shall, further to a reasoned request from a market surveillance authority, provide 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 *this Regulation* 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. Where the distributor of a product with digital elements becomes aware, *on the basis of information in its possession*, that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform, *without undue delay*, 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 21

Cases in which obligations of manufacturers apply to importers and distributors

An importer or distributor shall be considered to be a manufacturer for the purposes of this Regulation and shall be subject to **■** Articles 13 and *14*, where that importer or distributor places a product with digital elements on the market under *its* name or trademark or carries out a substantial modification of a product with digital elements already placed on the market.

Article 22

Other cases in which obligations of manufacturers apply

1. A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of a product with digital elements ***and makes that product available on the market***, shall be considered to be a manufacturer for the purposes of this Regulation.
2. The person referred to in paragraph 1 of this Article shall be subject to **■ *the obligations set out in*** Articles 13 and ***14*** for the part of the product ***with digital elements*** 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 23

Identification of economic operators

1. Economic operators shall, on request **■**, provide the market surveillance authorities *with* the following information:
 - (a) the name and address of any economic operator who has supplied them with a product with digital elements;
 - (b) where available, the 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 10 years after they have been supplied with the product with digital elements and for 10 years after they have supplied the product with digital elements.

Article 24

Obligations of open-source software stewards

- 1. Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject. That policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community.*

2. *Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software.*

Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.

3. *The obligations laid down in Article 14(1) shall apply to open-source software stewards to the extent that they are involved in the development of the products with digital elements. The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products.*

Article 25

Security attestation of free and open-source software

In order to facilitate the due diligence obligation set out in Article 13(5), in particular as regards manufacturers that integrate free and open-source software components in their products with digital elements, the Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by establishing voluntary security attestation programmes allowing the developers or users of products with digital elements qualifying as free and open-source software as well as other third parties to assess the conformity of such products with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation.

Article 26

Guidance

- 1. In order to facilitate implementation and ensure the consistency of such implementation, the Commission shall publish guidance to assist economic operators in applying this Regulation, with a particular focus on facilitating compliance by microenterprises and small and medium-sized enterprises.*
- 2. Where it intends to provide guidance as referred to in paragraph 1, the Commission shall address at least the following aspects:*
 - (a) the scope of this Regulation, with a particular focus on remote data processing solutions and free and open-source software;*
 - (b) the application of support periods in relation to particular categories of products with digital elements;*

(c) guidance targeted at manufacturers subject to this Regulation that are also subject to Union harmonisation legislation other than this Regulation or to other related Union legal acts;

(d) the concept of substantial modification.

The Commission shall also maintain an easy-to-access list of the delegated and implementing acts adopted pursuant to this Regulation.

3. When preparing the guidance pursuant to this Article, the Commission shall consult relevant stakeholders.

CHAPTER III
CONFORMITY OF THE PRODUCT WITH DIGITAL ELEMENTS

Article 27

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 cybersecurity requirements ***set out in Annex I*** covered by those standards or parts thereof.

The Commission shall, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the essential cybersecurity requirements set out in Annex I to this Regulation. When preparing standardisation requests for this Regulation, the Commission shall strive to take into account existing European and international standards for cybersecurity that are in place or under development in order to simplify the development of harmonised standards, in accordance with Regulation (EU) No 1025/2012.

2. The Commission may adopt implementing acts establishing common specifications covering technical requirements that provide a means to comply with the essential cybersecurity requirements set out in Annex I for products with digital elements that fall within the scope of this Regulation.

Those implementing acts shall be adopted only where the following conditions are 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 cybersecurity requirements set out in Annex I and:**
 - (i) the request has not been accepted;**
 - (ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or**
 - (iii) the harmonised standards do not comply with the request; and**

(b) no reference to harmonised standards covering the relevant essential cybersecurity requirements set out in Annex I has been 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.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

- 3. Before preparing the draft implementing act referred to in paragraph 2 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers that the conditions in paragraph 2 of this Article have been fulfilled.***
- 4. When preparing the draft implementing act referred to in paragraph 2, the Commission shall take into account the views of relevant bodies and shall duly consult all relevant stakeholders.***
- 5. Products with digital elements and processes put in place by the manufacturer which are in conformity with the common specifications established by implementing acts referred to in paragraph 2 of this Article, or parts thereof, shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I covered by those common specifications or parts thereof.***

6. *Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing 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 a reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the implementing acts referred to in paragraph 2, or parts thereof which cover the same essential cybersecurity requirements as those covered by that harmonised standard.*

7. *Where a Member State considers that a common specification does not entirely satisfy the essential cybersecurity requirements set out in Annex I, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.*

8. 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 *pursuant to* Regulation (EU) 2019/881 ■ , shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I in so far as the EU statement of conformity or *European* cybersecurity certificate, or parts thereof, cover those requirements.
9. The Commission is empowered *to adopt delegated acts in accordance with Article 61 of this Regulation 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 cybersecurity requirements or parts thereof as set out in Annex I to this Regulation. Furthermore, *the issuance of a European* cybersecurity certificate issued under such schemes, *at least at assurance level ‘substantial’*, eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 32(2), *points (a) and (b), and Article 32(3), points (a) and (b), of this Regulation.* ■

■

Article 28

EU declaration of conformity

1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 13(12) and state that the fulfilment of the applicable essential cybersecurity requirements set out in Annex I has been demonstrated.
2. The EU declaration of conformity shall have the model structure set out in Annex V and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VIII. Such a declaration shall be updated *as appropriate*. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available *on the market*.

The simplified EU declaration of conformity referred to in Article 13(20) shall have the model structure set out in Annex VI. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market.

3. Where a product with digital elements is subject to more than one Union *legal* act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union *legal* acts. That declaration shall contain the identification of the Union legal 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 *with digital elements*.
5. The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by adding elements to the minimum content of the EU declaration of conformity set out in Annex V to take account of technological developments.

Article 29

General principles of the CE marking

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

Article 30

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 28 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 28 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 ***cybersecurity*** 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 32.

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 Union harmonisation legislation *other than this Regulation* which also provides for the affixing of the CE marking, the CE marking shall indicate that the product also fulfils the requirements set out in *such other Union harmonisation* legislation.

6. The Commission may, by means of implementing acts, lay down technical specifications for *labels*, pictograms or any other marks related to the security of the products with digital elements, *their support periods* and mechanisms to promote their use *and to increase public awareness about the security of products with digital elements*. *When preparing the draft implementing acts, the Commission shall consult relevant stakeholders, and, if it has already been established pursuant to Article 52(15), ADCO*. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 31

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 cybersecurity requirements set out in Annex I. It shall at least contain the elements set out in Annex VII.

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, at least during *the support* period **■** .
3. For products with digital elements as referred to in Article 12, which are also subject to other Union *legal* acts *which provide for technical documentation*, a single set of technical documentation shall be drawn up containing the information referred to in Annex VII and the information required by those Union *legal* 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 61 to supplement this Regulation by *adding* elements to be included in the technical documentation set out in Annex VII to take account of technological developments, as well as developments encountered in the implementation process of this Regulation. *To that end, the Commission shall strive to ensure that the administrative burden on microenterprises and small and medium-sized enterprises is proportionate.*

Article 32

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 cybersecurity requirements set out in Annex I are met. The manufacturer ■ shall demonstrate conformity with the essential cybersecurity requirements by using *any* of the following procedures:
 - (a) the internal control procedure (based on module A) set out in Annex VIII; ■
 - (b) the EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII; ■
 - (c) a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; *or*
 - (d) *where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9).*

2. Where, in assessing the compliance of an *important* product with digital elements *that falls under* class I as set out in Annex III and the processes put in place by its manufacturer with the essential cybersecurity requirements set out in Annex I, the manufacturer **■** has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes *at assurance level at least ‘substantial’* as referred to in Article 27, 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 cybersecurity requirements to *any* of the following procedures:
- (a) *the* EU-type examination procedure (based on module B) *set out* in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII; or
 - (b) a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII.

3. Where the product is an *important* product with digital elements *that falls under* class II as set out in Annex III, the manufacturer ■ shall demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using *any* of the following procedures:
- (a) EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII; ■
 - (b) a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; *or*
 - (c) *where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9) of this Regulation at assurance level at least ‘substantial’ pursuant to Regulation (EU) 2019/881.*

4. *Critical products with digital elements listed in Annex IV shall demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using one of the following procedures:*
- (a) a European cybersecurity certification scheme in accordance with Article 8(1); or*
 - (b) where the conditions in Article 8(1) are not met, any of the procedures referred to in paragraph 3 of this Article.*
5. *Manufacturers of products with digital elements qualifying as free and open-source software, which fall under the categories set out in Annex III, shall be able to demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using one of the procedures referred to in paragraph 1 of this Article, provided that the technical documentation referred to in Article 31 is made available to the public at the time of the placing on the market of those products.*

6. ■ The specific interests and needs of *microenterprises and* small and *medium-sized* enterprises, *including start-ups, shall be taken into account* when setting the fees for conformity assessment procedures and ■ those fees *shall be reduced* proportionately to their specific interests and needs.

Article 33

Support measures for microenterprises and small and medium-sized enterprises, including start-ups

- 1. Member States shall, where appropriate, undertake the following actions, tailored to the needs of microenterprises and small enterprises:*
 - (a) organise specific awareness-raising and training activities about the application of this Regulation;*
 - (b) establish a dedicated channel for communication with microenterprises and small enterprises and, as appropriate, local public authorities to provide advice and respond to queries about the implementation of this Regulation;*
 - (c) support testing and conformity assessment activities, including where relevant with the support of the European Cybersecurity Competence Centre.*

2. *Member States may, where appropriate, establish cyber resilience regulatory sandboxes. Such regulatory sandboxes shall provide for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with this Regulation for a limited period of time before the placing on the market. The Commission and, where appropriate, ENISA, may provide technical support, advice and tools for the establishment and operation of regulatory sandboxes. The regulatory sandboxes shall be set up under the direct supervision, guidance and support by the market surveillance authorities. Member States shall inform the Commission and the other market surveillance authorities of the establishment of a regulatory sandbox through ADCO. The regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. Member States shall ensure open, fair, and transparent access to regulatory sandboxes, and in particular facilitate access by microenterprises and small enterprises, including start-ups.*

3. *In accordance with Article 26, the Commission shall provide guidance for microenterprises and small and medium-sized enterprises in relation to the implementation of this Regulation.*
4. *The Commission shall advertise available financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and small enterprises.*
5. *Microenterprises and small enterprises may provide all elements of the technical documentation specified in Annex VII by using a simplified format. For this purpose, the Commission shall, by means of implementing acts, specify the simplified technical documentation form targeted at the needs of microenterprises and small enterprises, including how the elements set out in Annex VII are to be provided. Where a microenterprise or small enterprise opts to provide the information set out in Annex VII in a simplified manner, it shall use the form referred to in this paragraph. Notified bodies shall accept that form for the purposes of conformity assessment.*

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 34

Mutual recognition agreements

Taking into account the level of technical development and the approach on conformity assessment of a third country, the Union may conclude Mutual Recognition Agreements with third countries, in accordance with Article 218 TFEU, in order to promote and facilitate international trade.

CHAPTER IV
NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

Article 35
Notification

1. Member States shall notify the Commission and the other Member States of **■** bodies authorised to carry out conformity assessments in accordance with this Regulation.
2. *Member States shall strive to ensure, by ... [24 months from the date of entry into force of this Regulation] 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.*

Article 36

Notifying authorities

1. Each Member State shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and their monitoring, including compliance with Article 41.
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.
3. ***Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 of this Article to a body which is not a governmental entity, that body shall be a legal entity and shall comply mutatis mutandis with Article 37. In addition, it shall have arrangements in place to cover liabilities arising from its activities.***
4. ***The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3.***

Article 37

Requirements relating to notifying authorities

1. A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs.
2. A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities.
3. A notifying authority shall be organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment.
4. A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis.
5. A notifying authority shall safeguard the confidentiality of the information it obtains.
6. A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.

Article 38

Information obligation on notifying authorities

1. Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes thereto.
2. The Commission shall make *the* information *referred to in paragraph 1* publicly available.

Article 39

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 *with digital elements* 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 *to be* such a third-party 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, *importer, distributor*, 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, *import, distribution*, the marketing, installation, use or maintenance of the products *with digital elements which they assess*, 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 VIII 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) *personnel* 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 *to be* carried out, ensuring the transparency of and ability to reproduce 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.

A conformity assessment body 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 cybersecurity requirements *set out in Annex I*, of the applicable harmonised standards *and common specifications*, and of the relevant provisions of Union harmonisation legislation and implementing acts;
 - (d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

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

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

9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by *their Member* 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 VIII or any provision of national law giving effect to it, except in relation to the market surveillance authorities of the Member State in which its activities are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.

11. Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 51 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, *proportionate* and reasonable terms and conditions, ***while avoiding unnecessary burden for economic operators***, in particular taking into account the interests of *microenterprises and small and medium-sized enterprises* in relation to fees.

Article 40

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 39 in so far as the applicable harmonised standards cover those requirements.

Article 41

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 39 and shall inform the notifying authority accordingly.
2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever they 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 42

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 *with digital elements* for which that body claims to be competent, as well as, *where applicable*, by an accreditation certificate issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 39.
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 39.

Article 43

Notification procedure

1. Notifying authorities shall notify only conformity assessment bodies which have satisfied the requirements laid down in Article 39.
2. The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations 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 *with digital elements* concerned and the relevant attestation of competence.
4. Where a notification is not based on an accreditation certificate as referred to in Article 42(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 39.

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 *to be 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 44

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 *legal 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 45
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 39, 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 46


Challenge of the competence of notified bodies

1. The Commission shall investigate all cases where it doubts, or *where* doubt is brought to its attention *regarding*, the competence of a notified body to meet, 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 47

Operational obligations of notified bodies

1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 32 and Annex VIII.
2. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for economic operators. Conformity assessment bodies shall perform their activities taking due account of the size of undertakings, ***in particular as regards microenterprises and small and medium-sized enterprises***, the sector in which ***they*** operate, ***their*** structure, their degree of complexity ***and the cybersecurity risk level*** of the products ***with digital elements 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 products ***with digital elements*** with the provisions of this Regulation.

4. Where a notified body finds that the requirements set out in Annex I or in corresponding harmonised standards or common specifications as referred to in Article 27 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a  certificate *of conformity*.
5. Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product *with digital elements* 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 48

Appeal against decisions of notified bodies

Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.

Article 49

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 digital elements* with relevant information on issues relating to negative and, *upon* request, positive conformity assessment results.

Article 50

Exchange of experience

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

Article 51

Coordination of notified bodies

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

CHAPTER V
MARKET SURVEILLANCE AND ENFORCEMENT

Article 52

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

1. Regulation (EU) 2019/1020 shall apply to 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. ***The market surveillance authorities designated under paragraph 2 of this Article shall also be responsible for carrying out market surveillance activities in relation to the obligations for open-source software stewards laid down in Article 24. Where a market surveillance authority finds that an open-source software steward does not comply with the obligations set out in that Article, it shall require the open-source software steward to ensure that all appropriate corrective actions are taken. Open-source software stewards shall ensure that all appropriate corrective action is taken in respect of their obligations under this Regulation.***
4. Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated ***pursuant to*** Article 58 of Regulation (EU) 2019/881 and exchange information on a regular basis. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 14 of this Regulation, the designated market surveillance authorities shall cooperate ***and exchange information on a regular basis with the CSIRTs designated as coordinators and*** ENISA.

5. *The market surveillance authorities may request a CSIRT designated as coordinator or ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 54, market surveillance authorities may request the CSIRT designated as coordinator or ENISA to provide an analysis to support evaluations of compliance of products with digital elements.*
6. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of Union harmonisation legislation *other than this Regulation*, and exchange information on a regular basis.
7. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing those authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 10 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.

8. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and ***technical resources, including, where appropriate, processing automation tools, as well as with*** human resources ***with the necessary cybersecurity skills*** to fulfil their tasks under this Regulation.
9. The Commission shall ***encourage and*** facilitate the exchange of experience between designated market surveillance authorities.
10. Market surveillance authorities may provide guidance and advice to economic operators on the implementation of this Regulation, with the support of the Commission ***and, where appropriate, CSIRTs and ENISA.***

11. *Market surveillance authorities shall inform consumers of where to submit complaints that could indicate non-compliance with this Regulation, in accordance with Article 11 of Regulation (EU) 2019/1020, and shall provide information to consumers on where and how to access mechanisms to facilitate reporting of vulnerabilities, incidents and cyber threats that may affect products with digital elements.*
12. *Market surveillance authorities shall facilitate, where relevant, the cooperation with relevant stakeholders, including scientific, research and consumer organisations.*
13. 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.

14. For products with digital elements *that fall within* the scope of this Regulation which are classified as high-risk AI systems *pursuant* to Article 6 of Regulation (EU) 2024/1689, the market surveillance authorities designated for the purposes of Regulation (EU) 2024/1689 shall be the authorities responsible for market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to Regulation (EU) 2024/1689 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 14 *of this Regulation*, with *the CSIRTs designated as coordinators and* ENISA. Market surveillance authorities designated pursuant to Regulation (EU) 2024/1689 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.

15. ADCO shall be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. ADCO shall be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of single liaison offices. *ADCO shall also address specific matters related to the market surveillance activities in relation to the obligations placed on open-source software stewards.*

16. *Market surveillance authorities shall monitor how manufacturers have applied the criteria referred to in Article 13(8) when determining the support period of their products with digital elements.*

ADCO shall publish in a publicly accessible and user-friendly form relevant statistics on categories of products with digital elements, including average support periods, as determined by the manufacturer pursuant to Article 13(8), as well as provide guidance that includes indicative support periods for categories of products with digital elements.

Where the data suggests inadequate support periods for specific categories of products with digital elements, ADCO may issue recommendations to market surveillance authorities to focus their activities on such categories of products with digital elements.

Article 53

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 cybersecurity requirements set out in Annex I, the market surveillance authorities shall, ***upon a reasoned request***, be granted access to the data, ***in a language easily understood by them***, required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the ***relevant*** economic operator.

Article 54

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 *reason* to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall, ***without undue delay and, where appropriate, in cooperation with the relevant CSIRT***, carry out an evaluation of the product with digital elements concerned in respect of its compliance with all the requirements laid down in this Regulation. The relevant economic operators shall cooperate as necessary with the market surveillance authority.

Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant *economic* operator to take all appropriate corrective actions to bring the product ***with digital elements*** 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 *cybersecurity* risk, as ***the market surveillance authority*** may prescribe.

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

2. ***When determining the significance of a cybersecurity risk referred to in paragraph 1 of this Article, the market surveillance authorities shall also consider non-technical risk factors, in particular those established as a result of Union level coordinated security risk assessments of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555. Where a market surveillance authority 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 competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary.***
3. 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 ***economic*** operator to take.

4. The *economic operator* 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.
5. Where the *economic operator* 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 *with digital elements from* being made available on its national market, to withdraw it from that market or to recall it.

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

6. The information referred to in paragraph 5 shall include all available details, in particular the data necessary for the identification of the non-compliant **product** with digital elements, the origin of **that** 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 **economic** 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 **with digital elements** or of the processes put in place by the manufacturer to meet the essential cybersecurity requirements set out in Annex I;
 - (b) shortcomings in the harmonised standards, **European** cybersecurity certification schemes, or common specifications, as referred to in Article 27.
7. 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 **with digital elements** concerned, and, in the event of disagreement with the notified national measure, of their objections.

8. Where, within three months of receipt of the *notification* referred to in paragraph 5 *of this Article*, 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 to be justified. This is without prejudice to the procedural rights of the *economic* operator concerned in accordance with Article 18 of Regulation (EU) 2019/1020.
9. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product *with digital elements* concerned, such as withdrawal of *that* product from their market, without delay.

Article 55

Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 54(5), 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 *law*, 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 54(5) and notify *that* decision to the Member State concerned.
2. If the national measure is considered *to be* 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 not considered *to be* justified, the Member State concerned shall withdraw the measure.

3. Where the national measure is considered to be 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 **11** of Regulation (EU) No 1025/2012.
4. Where the national measure is considered to be 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 27, the Commission shall consider whether to amend or repeal any *delegated act adopted pursuant to* Article 27(9) that specifies the presumption of conformity concerning that certification scheme.
5. Where the national measure is considered to be justified and the non-compliance of the product with digital elements is attributed to shortcomings in common specifications as referred to in Article 27, the Commission shall consider whether to amend or repeal any implementing act *adopted pursuant to* Article 27(2) setting out those common specifications.

Article 56

Procedure at *Union* 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 *does not comply* with the requirements laid down in this Regulation, it *shall inform* the relevant market surveillance authorities. *Where the market surveillance authorities* carry out an evaluation of *that product with digital elements that may present a significant cybersecurity risk in respect of its compliance with the requirements laid down in this Regulation*, the procedures referred to in *Articles 54 and 55 shall apply*.

2. *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, where appropriate, the competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary. The Commission shall also consider the relevance of the identified risks for that product with digital elements in view of its tasks regarding the Union level coordinated security risk assessments of critical supply chains provided for in Article 22 of Directive (EU) 2022/2555, and consult as necessary the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and ENISA.*

3. In **■** circumstances which justify an immediate intervention to preserve the *proper* functioning of the internal market and where the Commission has sufficient reason to consider that the product *with digital elements* 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 carry out an evaluation of compliance and* may request ENISA to *provide an analysis to support it*. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

4. Based on *the* evaluation *referred to in paragraph 3*, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To that end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.
5. On the basis of the consultation referred to in paragraph 4 *of this Article*, the Commission may adopt implementing acts to *provide for* corrective or restrictive measures at Union level, including *requiring the products with digital elements concerned to be withdrawn* from the market or recalled, 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 62(2).
6. The Commission shall immediately communicate the *implementing acts* referred to in paragraph 5 to the relevant economic operator or operators. Member States shall implement *those implementing* acts without delay and shall inform the Commission accordingly.
7. Paragraphs 3 to 6 *shall be* applicable for the duration of the exceptional situation that justified the Commission's intervention, *provided that* the product *with digital elements concerned* is not brought in compliance with this Regulation.

Article 57

Compliant products with digital elements which present a significant cybersecurity risk

1. **█** The market surveillance authority of a Member State *shall require an economic operator to take all appropriate measures where, having performed an evaluation under Article 54, it finds that although a product with digital elements and the processes put in place by the manufacturer are in compliance with this Regulation, it presents a significant cybersecurity risk as well as a risk to:*
 - (a) *the health or safety of persons;*
 - (b) *the compliance with obligations under Union or national law intended to protect fundamental rights;*
 - (c) *the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555; or*
 - (d) *other aspects of public interest protection.*

The measures referred to in the first subparagraph may include measures to ensure that the product with digital elements concerned and the processes put in place by the manufacturer no longer present the relevant risks when made available on the market, withdrawal from the market of the product with digital elements concerned, or recalling of it, and shall be commensurate with the nature of those risks.

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 *the* decision *referred to in paragraph 4* to the Member States.
6. Where the Commission has sufficient *reason* 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 *of this Article*, it *shall inform and* may request the relevant market surveillance authority or authorities to carry out an evaluation ■ and follow the procedures referred to in Article 54 and paragraphs 1, 2 and 3 of this Article.

7. In **■** circumstances which justify an immediate intervention to preserve the *proper* functioning of the internal market and where the Commission has sufficient reason to consider that the product *with digital elements* 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 *shall* carry out an evaluation of the risks presented by that product *with digital elements and may request ENISA to provide an analysis to support that evaluation* and shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.
8. Based on *the* evaluation referred to in paragraph 7, the Commission may establish that a corrective or restrictive measure is necessary at Union level. To that end, it shall without delay consult the Member States concerned and the relevant *economic* operator or operators.

9. On the basis of the consultation referred to in paragraph 8 of this Article, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including *requiring the products with digital elements concerned to be withdrawn* from the market, or recalled, 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 62(2).
10. The Commission shall immediately communicate the *implementing acts* referred to in paragraph 9 to the relevant *economic* operator or operators. Member States shall implement *those implementing* 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 *product with digital elements concerned* continues to present the risks referred to in paragraph 1.

Article 58

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 put an end to the non-compliance concerned:
 - (a) the **CE** marking has been affixed in violation of Articles 29 and 30;
 - (b) the **CE** 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 59

Joint activities of market surveillance authorities

1. Market surveillance authorities may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and the protection of consumers with respect to specific products with digital elements placed *on the market* or made available on the market, in particular products *with digital elements* 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 *with digital elements that fall within* the scope of this Regulation with the requirements laid down *in this Regulation*.
3. The market surveillance authorities and **■**, where applicable, *the Commission*, 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 *obtained as a result of the joint* activities carried out as part of any investigation that it undertakes.
5. The market surveillance authority concerned and, *where applicable, the Commission*, shall make the agreement on joint activities, including the names of the parties involved, available to the public.

Article 60

Sweeps

1. Market surveillance authorities *shall* 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. *Those sweeps may include inspections of products with digital elements acquired under a cover identity.*
2. Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep *shall*, where appropriate, make the aggregated results publicly available.

3. **Where**, in the performance of its tasks, including based on the notifications received pursuant to Article 14(1) and (3), **ENISA identifies** categories of products **with digital elements** for which sweeps may be organised, **it shall submit a proposal for a sweep** to the **coordinator** referred to in paragraph 2 **of this Article** 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 52 to 58 and any other powers conferred upon them by national law.
5. Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.

CHAPTER VI
DELEGATED POWERS AND COMMITTEE PROCEDURE

Article 61

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(5), second subparagraph, Article 7(3), Article 8(1) and (2), Article 13(8), fourth subparagraph, Article 14(9), Article 25, Article 27(9), Article 28(5) and Article 31(5) shall be conferred on the Commission *for a period of five years from ... [date of entry into force of this Regulation]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.*

3. The delegation of power referred to in Article 2(5), *second subparagraph*, Article 7(3), Article 8(1) and (2), Article 13(8), *fourth subparagraph*, Article 14(9), Article 25, Article 27(9), Article 28(5) and Article 31(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 *Interinstitutional* 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(5), second subparagraph, Article 7(3), Article 8(1) or (2), *Article 13(8), fourth subparagraph, Article 14(9)*, Article 25, *Article 27(9)*, Article 28(5) or Article 31(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 62
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 63
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 (EU) 2016/943 of the European Parliament and of the Council³⁶;
 - (b) the effective implementation of this Regulation, in particular for the purposes of inspections, investigations or audits;
 - (c) public and national security interests;
 - (d) integrity of criminal or administrative proceedings.

³⁶ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

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 64

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements **■** of this Regulation and shall take all measures necessary to ensure that they are *implemented*. The penalties provided for shall be effective, proportionate and dissuasive. ***Member States shall, without delay, notify the Commission of those rules and measures and shall notify it, without delay, of any subsequent amendment affecting them.***

■

2. Non-compliance with the essential cybersecurity requirements set out in Annex I and the obligations set out in Articles 13 and 14 shall be subject to administrative fines of up to EUR 15 000 000 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.

3. Non-compliance with *the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53* shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.
4. 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 EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.
5. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:
 - (a) the nature, gravity and duration of the infringement and of its consequences;

- (b) whether administrative fines have been already applied by *the same or* other market surveillance authorities to the same *economic* operator for a similar infringement;
 - (c) the size, *in particular with regard to microenterprises and small and medium sized-enterprises, including start-ups*, and *the* market share of the *economic* operator committing the infringement.
6. Market surveillance authorities that apply administrative fines shall *communicate that application to* the market surveillance authorities of other Member States through the information and communication system referred to in Article 34 of Regulation (EU) 2019/1020.
7. Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and *public* bodies established in that Member State.

8. 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.
9. 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.
10. ***By way of derogation from paragraphs 3 to 9, the administrative fines referred to in those paragraphs shall not apply to the following:***
- (a) manufacturers that qualify as microenterprises or small enterprises with regard to any failure to meet the deadline referred to in Article 14(2), point (a), or Article 14(4), point (a);***
 - (b) any infringement of this Regulation by open-source software stewards.***

Article 65

Representative actions

Directive (EU) 2020/1828 shall apply to the representative actions brought against infringements by economic operators of provisions of this Regulation that harm, or may harm, the collective interests of consumers.

CHAPTER VIII
TRANSITIONAL AND FINAL PROVISIONS

Article 66

Amendment to Regulation (EU) 2019/1020

In Annex I to Regulation (EU) 2019/1020 the following point is added:

‘XX⁺. Regulation (EU) 2024/... of the European Parliament and of the Council*⁺⁺.

* ***Regulation (EU) 2024/... of the European Parliament and of the Council of ... on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ ..., ELI: ...).***

⁺ OJ: Please insert in the text the next consecutive number of the list in Annex I to Regulation (EU) 2019/1020.

⁺⁺ ***OJ: Please insert in the text the number of the Regulation contained in document PE-CONS 100/23 (2022/0272(COD)) and insert the number, date and OJ reference of that Regulation in the footnote.***

Article 67

Amendment to Directive (EU) 2020/1828

In Annex I to Directive (EU) 2020/1828 the following point is added:

'(XX⁺) Regulation (EU) 2024/... of the European Parliament and of the Council⁺⁺.*

** Regulation (EU) 2024/... of the European Parliament and of the Council of ... on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ..., ELI: ...).'*

⁺ OJ: Please insert in the text the next consecutive number of the list in Annex I to Directive (EU) 2020/1828.

⁺⁺ *OJ: Please insert in the text the number of the Regulation contained in document PE-CONS 100/23 (2022/0272(COD)) and insert the number, date and OJ reference of that Regulation in the footnote.*

Article 68

Amendment to Regulation (EU) No 168/2013

Annex II to Regulation (EU) No 168/2013 of the European Parliament and of the Council³⁷ is amended as follows:

In Part C1, in the table, the following entry is added:

‘

XX ⁺	18	<i>Protection of vehicle against cyberattacks</i>		x	x	x	x	x	x	x	x	x	x	x	x	x	x
-----------------	----	---	--	---	---	---	---	---	---	---	---	---	---	---	---	---	---

’

³⁷ *Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).*

⁺ OJ: Please insert in the text the next consecutive number under heading C1 in Annex II to Regulation (EU) No 168/2013.

Article 69

Transitional provisions

1. EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for products with digital elements that are subject to Union harmonisation legislation *other than this Regulation* shall remain valid *until ...* [42 months *from* the date of entry into force of this Regulation], unless they expire before that date, or unless otherwise specified in *such* other Union *harmonisation* legislation, in which case they shall remain valid as referred to in that *legislation*.
2. Products with digital elements that have been placed on the market before ... [**36 months from the date of entry into force of this Regulation**] shall be subject to the requirements set out in this Regulation only if, from that date, those products are subject to a substantial modification **■** .
3. By way of derogation from paragraph 2 of this Article, the obligations laid down in Article 14 shall apply to all products with digital elements *that fall* within the scope of this Regulation that have been placed on the market before ... [**36 months from the date of entry into force of** this Regulation].

Article 70

Evaluation and review

1. By ... [72 months **from** the date of entry into force 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. Those reports shall be made public.
2. ***By ... [45 months from the date of entry into force of this Regulation], the Commission shall, after consulting ENISA and the CSIRTs network, submit a report to the European Parliament and to the Council, assessing the effectiveness of the single reporting platform set out in Article 16, as well as the impact of the application of the cybersecurity-related grounds referred to Article 16(2) by the CSIRTs designated as coordinators on the effectiveness of the single reporting platform as regards the timely dissemination of received notifications to other relevant CSIRTs.***

Article 71

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. ***This Regulation*** shall apply from ... [**36 months *from*** the date of entry into force of this Regulation].

However, Article 14 shall apply from ... [**21 months *from*** the date of entry into force of this Regulation] and ***Chapter IV (Articles 35 to 51)*** shall apply from ... [**18 months *from 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
The President

For the Council
The President

Annex I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I *Cybersecurity* requirements relating to the properties of products with digital elements

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



- (2) On the basis of the *cybersecurity* risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

- (a) *be made available on the market without known exploitable vulnerabilities;*
- (b) be *made available on the market* with a secure by default configuration, *unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements*, including the possibility to reset the product to its original state;

- (c) *ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;*
- (d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, *and report on possible unauthorised access;*
- (e) 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;*

- (f) 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, **and** report on corruptions;
- (g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended **purpose** of the product **with digital elements** (data minimisation);
- (h) protect the availability of essential **and basic** functions, **also after an incident**, including **through** resilience ■ and mitigation **measures against** denial-of-service attacks;
- (i) minimise **the** negative impact **by the products themselves or connected devices** on the availability of services provided by other devices or networks;
- (j) be designed, developed and produced to limit attack surfaces, including external interfaces;

- (k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
- (l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, *with an opt-out mechanism for the user*;
- (m) *provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.*

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

- (1) identify and document vulnerabilities and components contained in products *with digital elements*, 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 products;

- (2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; ***where technically feasible, new security updates shall be provided separately from functionality updates;***
- (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, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and ***clear and accessible*** information helping users to remediate the vulnerabilities; ***in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;***
- (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 updates for products with digital elements to ensure that ■ vulnerabilities are fixed or mitigated in a timely *manner and, where applicable for security updates, in an automatic* manner;
- (8) ensure that, where security ■ updates are available to address identified security issues, they are disseminated without delay and, *unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements*, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Annex II

INFORMATION AND INSTRUCTIONS TO THE USER

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

1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, ■ the email address *or other digital contact as well as, where available, the website at which the manufacturer can be contacted*;
2. the *single* point of contact where information about ■ vulnerabilities of the product *with digital elements* can be reported and received, *and where the manufacturer's policy on coordinated vulnerability disclosure can be found*;
3. *name and type and any additional information enabling the unique* identification of the product *with digital elements* ■ ;
4. the intended *purpose of the product with digital elements*, 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. where applicable, the internet address at which the EU declaration of conformity can be accessed;

7. the type of technical security support offered by the manufacturer and ***the end-date of the support period during which users can expect vulnerabilities to be handled and*** to receive security updates;

8. 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 ***with digital elements*** to ensure its secure use;

(b) how changes to the product ***with digital elements*** can affect the security of data;

- (c) how security-relevant updates can be installed;
- (d) the secure decommissioning of the product *with digital elements*, including information on how user data can be securely removed;
- (e) *how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;*
- (f) *where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.*

9. *If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.*

IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS

■ Class I

1. Identity management systems ■ and privileged access management software *and hardware, including authentication and access control readers, including biometric readers*;
2. Standalone and embedded browsers;
3. Password managers;
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. Security information and event management (SIEM) systems;

8. ■ Boot managers;

■

9. *Public key infrastructure and digital certificate issuance software;*

10. Physical *and virtual* network interfaces;

11. Operating systems ■ ;

■

12. Routers, modems intended for the connection to the internet, and switches ■ ;

13. Microprocessors *with security-related functionalities;*

14. Microcontrollers *with security-related functionalities;*

15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) *with security-related functionalities;*

■

16. *Smart home general purpose virtual assistants;*

17. *Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems;*

18. *Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council¹ that have social interactive features (e.g. speaking or filming) or that have location tracking features;*
19. *Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply, or personal wearable products that are intended for the use by and for children.*

■ Class II

■

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

■

2. Firewalls, intrusion detection and prevention systems ■ ;

3. *Tamper-resistant* microprocessors;

4. *Tamper-resistant microcontrollers.*

■

¹ *Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1).*

Annex IV

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

1. ***Hardware Devices with Security Boxes;***
2. ***Smart meter gateways within smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 of the European Parliament and of the Council¹ and other devices for advanced security purposes, including for secure cryptoprocessing;***
3. ***Smartcards or similar devices, including secure elements.***

¹ ***Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).***

Annex V

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 28, 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 its 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 *with digital elements* allowing traceability, *which* 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 VI

SIMPLIFIED EU DECLARATION OF CONFORMITY

The simplified EU declaration of conformity referred to in Article 13(20) shall be provided as follows:

Hereby, [Name of manufacturer] declares that the product with digital elements type [designation of type of product with digital element] is in compliance with Regulation (EU) .../... of the European Parliament and of the Council².

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

² *OJ: Please insert in the text the number of the Regulation contained in document PE-CONS No/YY (2022/0272(COD)).*

Annex VII

CONTENTS OF THE TECHNICAL DOCUMENTATION

The technical documentation referred to in Article 31 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 cybersecurity 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 *with digital elements* and vulnerability handling processes, including:
 - (a) *necessary* information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;

- (b) **necessary** 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) **necessary** information and specifications of the production and monitoring processes of the product with digital elements and the validation of *those* processes;
3. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, **including how the essential cybersecurity requirements set out in Part I of Annex I are applicable**;
 4. **relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements**;

5. 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 27 of this Regulation or **European** cybersecurity certification schemes **adopted pursuant to** Regulation (EU) 2019/881 pursuant to Article 27(8) **of this Regulation**, and, where those harmonised standards, common specifications or **European** cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential cybersecurity requirements set out in Parts I and II of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or **European** cybersecurity certification **schemes**, the technical documentation shall specify the parts which have been applied;
6. reports of the tests carried out to verify the conformity of the product **with digital elements** and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I;
7. a copy of the EU declaration of conformity;
8. where applicable, the software bill of materials, 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 cybersecurity requirements set out in Annex I.

Annex VIII

CONFORMITY ASSESSMENT PROCEDURES

Part I ■ 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 set out in points 2, 3 and 4 of this Part, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential cybersecurity requirements set out in Part I of Annex I and the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.
2. The manufacturer shall draw up the technical documentation described in Annex VII.
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 cybersecurity requirements set out in Parts I and II of Annex I.

4. Conformity marking and declaration of conformity

4.1. The manufacturer shall affix the CE **marking** to each individual product with digital elements that satisfies the applicable requirements set out in 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 28 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 for 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 **its** authorised representative, on **its** behalf and under **its** responsibility, provided that the relevant obligations are specified in the mandate.

Part II ■ 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 *with digital elements* and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II 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 *with digital elements* 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 *its* choice.

The application shall include:

- 3.1 the name and address of the manufacturer and, if the application is lodged by the authorised representative, *its* name and address as well;
- 3.2 a written declaration that the same application has not been lodged with any other notified body;
- 3.3 the technical documentation, which shall make it possible to assess the conformity *of the product with digital elements* with the applicable essential cybersecurity requirements as set out in Part I of Annex I and the manufacturer's vulnerability handling processes set out in Part II of Annex I and shall include an adequate analysis and assessment of the risks. 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 *with digital elements*. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex VII;

3.4 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 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 its behalf and under *its* 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 digital elements* with the essential cybersecurity requirements set out in Part I of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I;

- 4.2. verify that specimens 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 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 that, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I, they have been applied correctly;
- 4.4. carry out appropriate examinations and tests, or have them carried out, to check that, where the solutions in the relevant harmonised standards 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 cybersecurity 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 cybersecurity 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 digital elements* 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 cybersecurity 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 cybersecurity 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 cybersecurity 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. ***The notified body shall carry out periodic audits to ensure that the vulnerability handling processes as set out in Part II of Annex I are implemented adequately.***

9. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and 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 any additions thereto refused, suspended or otherwise restricted.

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

- 10.** 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 *with digital elements* has been placed on the market *or for the support period, whichever is longer*.
- 11.** The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 10, provided that the relevant obligations are specified in the mandate.

Part III ■ 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 set out in points 2 and 3 of this Part, and ensures and declares that the products *with digital elements* concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential cybersecurity requirements set out in Part I of Annex I *and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I*.

2. Production

The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products *with digital elements* with the approved type described in the EU-type examination certificate and with the essential cybersecurity requirements as set out in Part I of Annex I *and ensures that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.*

3. Conformity marking and declaration of conformity

- 3.1. The manufacturer shall affix the CE marking to each individual product *with digital elements* that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements set out in 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 *with digital elements* has been placed on the market *or for the support period, whichever is longer*. 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 *its* authorised representative, on *its* behalf and under *its* responsibility, provided that the relevant obligations are specified in the mandate.

Part IV ■ Conformity based on full quality assurance (based on Module H)

- I.* Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 5 of this Part, and ensures and declares on its sole responsibility that the products *with digital elements* or product categories concerned satisfy the essential cybersecurity requirements set out in Part I of Annex I and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Part II 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 final product inspection and testing** of the products **with digital elements** concerned and for handling vulnerabilities, maintain its effectiveness throughout **the support period**, 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 its quality system with the notified body of its choice, for the products **with digital elements** concerned.

The application shall include:

- the name and address of the manufacturer and, if the application is lodged by the authorised representative, **its** name and address as well;

- the technical documentation for one model of each category of products *with digital elements* intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in Annex VII;
 - 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 digital elements* with the essential cybersecurity requirements set out in Part I of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Part II 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 or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part I of Annex I that apply to the products *with digital elements* will be met;
- the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part II 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 *with digital elements* 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 *and* qualification reports on the personnel concerned;
- 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 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 *shall have* knowledge of the applicable requirements set out in 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 set out in this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product *with digital elements* with those requirements.

The manufacturer or its 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 *and* tests;
- the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data *and* qualification reports on the personnel concerned.

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 *with digital elements* that satisfies the requirements set out in Part I 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 *with digital elements* has been placed on the market *or for the support period, whichever is longer*. 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 *with digital elements* has been placed on the market *or for the support period, whichever is longer*, keep at the disposal of the national authorities:

6.1 the technical documentation referred to in point 3.1;

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

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

6.4 the decisions and reports of the notified body referred to in points 3.5 *and* 4.3.

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 *its* authorised representative, on *its* behalf and under *its* responsibility, provided that the relevant obligations are specified in the mandate.

A statement has been made with regard to this act and can be found in [OJ office to provide: OJ C, XXX, XX.XX.2024, p. XX] and at the following link: [OJ office: please insert the link to the statement].

Joint political statement by the European Parliament, the Council and the Commission on ENISA resources, on the occasion of the adoption of Regulation (EU) .../...of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*

The European Parliament and the Council consider that this Regulation confers additional tasks on ENISA which result in additional workload and would require additional resources in terms of both expertise and number. In view of this, in order to enable ENISA to effectively carry out the tasks under this Regulation, the European Parliament, the Council and the Commission consider that an increase in its resources, in particular its human resources with the adequate expertise, may be necessary. Such increase could be provided for in the annual procedure related to the establishment plan of ENISA. Accordingly, the Commission, which is responsible for entering in the draft general budget of the Union the estimates it deems to be necessary for ENISA's establishment plan, in the framework of the budgetary procedure set out in Article 314 TFEU and in accordance the procedure set out in the Cybersecurity Act, shall assess the estimates for the establishment plan of ENISA entered for the first year after entry into force of this Regulation in consideration of the necessary resources, in particular human resources, to enable ENISA to adequately carry out its tasks under this Regulation.

** [The provisional political agreement concluded to have this statement published in the C-Series of the Official Journal and to have a reference and a link to them in the L-Series, together with the legislative act.]*