Council of the European Union
General Secretariat

Brussels, 04 May 2023

WK 5771/2023 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	General Secretariat of the Council
To:	Delegations
N° prev. doc.:	WK 5175/23
N° Cion doc.:	ST 12429 2022 + ADD 1-6
Subject:	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - Delegations' comments

Delegations will find in the Annex the comments from DK, DE, IT, HU, NL and FI on the above-mentioned legislative proposal set out in WK 5175/2023.

Table of Contents

Denmark

General comments

We would like to express our gratitude to the Presidency for the new compromise text. Overall, we find the new proposal to be a step in the right direction; improving the clarity of the scope and the alignment with relevant EU acquis.

In our view, while there are many details throughout the text, which could still be improved, the major remaining challenges concerns articles 2, 4, 6, 6a and 11, Annex III and their related recitals.

Article 2 - Scope

We continue to be concerned that the exclusion clause – as currently phrased – could hamper Member States' ability to exercise their responsibilities for national security and defence sufficiently – more specifically we have some concerns about dual use. As suggested in our previous written comments, we believe it is necessary to add some flexibility for authorities carrying out functions related to national security, defence or military purposes. We are looking into whether the exclusion clause in the AI act can be used and will provide a textual compromise proposal in this regard soon.

Article 3 – Definitions

We suggest defining 'common specifications', similarly to the one proposed in the Council's general approach in the Data Act:

(New) (i)	**'common specifications' means a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation;**

Article 4 – Free movement

Denmark supports the current approach to establish horizontal minimum cybersecurity rules based on the principles of maximum harmonization in the internal market. However, we continue to have concerns regarding member states' ability to impose restrictions or prohibitions against the use of certain products that comply with the CRA, or to prohibit maintaining or entering into an agreement regarding critical network components, to safeguard national security. It is absolutely necessary that Member States are able to take considerations regarding national security into account through national regulation.

We welcome the new recital corresponding to Art. 4, para 1. Moreover, we welcome that the Commission confirmed at the meeting in HWPCI on 16 March, that the intention with the CRA is not to limit Member States in their right to subject products to additional measures. However, we find it necessary to clarify that Member States should be able subject products with digital elements to additional measures. Measures should include

the prohibition of the use of such products or of entering into or upholding agreements concerning the purchase, management of operations or support of such products, in accordance with national law.

Therefore, we propose the following new compromise text to Art. 4, para 5, which, as we see it, also considers some of the concerns raised by other Member States regarding national special regulation. Our proposal is sector neutral.

> 5. *"This Regulation shall not apply to situations whereby Member States subject products with digital elements, or agreements concerning the purchase, management of operations and support of such products, to additional measures, including prohibition of use of the product and prohibition of entering into or upholding of such agreements, in accordance with national law."*

Article 6 – Classification of products with digital elements subject to specific conformity assessment procedures

Our general position remains that the proposal would be clearer, easier to implement and more fit for purpose if we removed article 6 and Annex III entirely. This would provide a solid basis on which to build future EU cybersecurity product legislation.

However, in the spirit of trying to find a practical compromise, we have previously suggested modifying Art. 6 by removing the class I and class II approach, leaving one category of products to be subject to the conformity assessment procedures originally prescribed to class I. Under what is now article 6a, the Commission could designate products, which would be required to undergo certification in accordance with assurance level substantial or high under the CSA. This would be more aligned with the general practice and need to subject products, which are more critical to safety and security, to a stricter set of requirements – not just different assessment procedures.

However, we do see the changes, introduced by the Presidency in the latest compromise text, as going in the right direction. Concerning this text, we have the following comments:

Article 6(2)

Currently, the text could give the impression that *all* products with digital elements should be divided into class I or II. To clarify, we propose that the first sentence in para 2 is aligned with the new title of the article to read:

> "Categories of products with digital elements**, which are subject to specific conformity assessment procedures,** are divided into class I and class II as set out in Annex III."

The last sentence of recital 25 and the middle sentence introduced in recital 26 should be aligned with the Presidency's changes in article 6(2)(a). Here, the term "primary function" has been introduced – which we strongly support. Therefore, the last sentence in recital 25 should read:

> "...the product ***primarily*** performs a central system function, including..."

Likewise, in the new middle sentence in recital 26, the word "primarily" should be added:

> "The categories of products with digital elements listed in class I of Annex III either have a cybersecurity related functionality or **primarily** perform**s** a central system function..."

Further, in regard to both of these recitals and art. 6(2)(a), we note that most products with digital elements have – or will have because of the CRA – *"cybersecurity-related functionality"*. For example, to authenticate and manage access to the devices itself or its associated software. As the text is worded now, all products with digital elements could therefore potentially meet the criteria. Therefore, we suggest the following revision:

> (a) "the product with digital elements ~~**has a cybersecurity-related functionality, and in particular**~~ performs primarily functions critical to **the** security **of other products or systems**, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;

In Art. 6(2)(b) the "*or*" between "*personal data*" and "*functions*" is confusing. Since the listing or functions refers to the "central system function", then "functions" appears to be connected to the second half of the sentence, by which the "or" is dividing it into two separate criteria. If this is intentional, then the second half should be point (c) – which we would oppose. Rather, we suggest deleting "or functions", since it is superfluous. Furthermore, we would like to simplify and reintroduce wording from the now deleted para 3(d) to account for damage done to people as well. Art. 6(2)(b) would then read:

> (b) the product with digital elements performs a central system function, including network management, configuration control, virtualisation, processing of personal data, ~~or functions~~ and has ~~a~~ the potential to ~~disrupt, control or damage a large number of other products with digital elements~~ have an adverse impact, in particular in terms of its intensity and its ability to affect a large number of persons and products, through direct manipulation.

Article 6(3) and (4)

With the latest changes, there appears to be no restrictions on the Commissions powers to amend the categories of article 6 nor the list of products in Annex III, beyond the requirement to take "*the function of the products*" into account.

We strongly oppose this. At a minimum, the para(s) should refer back to the criteria listed in para 2. Further, the delegation should be limited in time, cf. art. 50(2). We suggest a 5 years renewal clause, which is common practice in such legislation.

Annex III - Classes and categories of products with digital elements

Firstly, the title of the annex should be aligned with the changes in Art. 6, i.e.:

> "Classes and categories of products with digital elements **subject to specific conformity assessment procedures**"

Secondly, we are happy to see that the list has been reduced. However, we would still like to have it deleted entirely. Failing that, it should be cut further, or at a minimum the product groups should be specified in more detail to ensure that unintentional and unnecessary burdens are imposed.

For example, we do not find that 'Smart Meters' as a whole are appropriate under class II. In particular, with the changes made to articles 2 and 4 and the related new recital, allowing for special circumstances pertaining to national security, we find its placement here unnecessary and propose that it is deleted or moved to class I.

Article 11 - Reporting obligations of manufacturers

We find that reporting, which is the subject of article 11 of the CRA, should solely concern vulnerabilities for which patches exist. Reporting of unpatched vulnerabilities is an unnecessary safety risk. In particular, if reporting is done through a single platform and notifications are collected by ENISA. Such a single platform (or ENISA) risk becoming a target of malicious activities, which may have grave consequences for the Member States.

Recital 18

We thank the presidency for the clarification and shortening of recital 18. However, because the phrase "this Regulation", referring to the CRA's scope, has been removed, the current text could be interpreted to mean that if a product is in scope of eIDAS, then it automatically means that the CRA is also applicable. Keeping in mind the exemption of products from public authorities, this is not necessarily the case. We therefore find that "this Regulation" should be reinstated, to make it clear that in order for both the eIDAS regulation and CRA to be applicable, products have to fall into the scope of both regulations:

> 18) "To the extent that their products with digital elements fall within the scope of **this Regulation and** Regulation (EU) No 910/2014..."

Article 18

We appreciate the changes made regarding the provisions on common specifications. Recital 41 now fully reflects our understanding of what has been agreed in the Machinery Regulation. The changes made to article 18 are likewise positive, and the text is moving in the right direction. Yet, there are still some changes necessary for

the article to reflect the formulation from the Machinery Regulation fully, where a recent trilogue-agreement has been reached.

Below is the formulation in the abovementioned agreement on common specifications:

> 1. The Commission is empowered to adopt implementing acts, establishing common technical specifications for the essential cybersecurity requirements set out in Annex I, where the following conditions have been fulfilled:
>
>   (a) the Commission has requested, pursuant to Article 10(1) of Regulation 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the essential cybersecurity requirements set out in Annex 1 and the request has not been accepted or the European standardisation deliverables addressing that request is not delivered within the deadline set in accordance with Article 10(1) of Regulation 1025/2012 or European standardisation deliverables does not comply with the request, and;
>
>   (b) no reference to harmonised standards covering the relevant essential cybersecurity requirements set out in Annex 1 is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.
>
>   (c) Those implementing acts shall be adopted in accordance with the examination procedure referred to in article 51(2)
>
> 2. Before preparing a draft implementing act, 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 1 are fulfilled.
>
> 3. In the early preparation of the draft implementing act establishing the common specification, the Commission shall gather the views of relevant bodies or expert groups established under relevant sectorial Union law. Based on that consultation, the Commission shall prepare the draft implementing act.
>
> 4. When references of a harmonised standard are published in the Official Journal of the European Union, implementing acts referred to in paragraph 1, which cover the requirements set out Annex I, shall be repealed.
>
> 5. When a Member State considers that a common specification does not entirely satisfy the requirements set out in Annex I, it shall inform the Commission thereof with a detailed explanation and the Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification in question.
>
> 6. Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify in the technical documentation referred to in [Article 23] that they have adopted technical solutions that are at least equivalent thereto.

We wonder why the above text from the Machinery Regulation has not been fully incorporated and repeat our suggestion to introduce the agreed wording fully into the CRA.

Thank you for considering our comments. We look forward to continuing the constructive discussions on the file.

Germany

[…]

(New recital corresponding to Art 4, para 1)

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 further requirements for the making available on the market of products with digital elements. Member States or Entities can however establish or maintain additional requirements to those laid down by this Regulation for the procurement or use of those products for their 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. Furthermore, Directive (EU) 2022/2555 sets out cybersecurity risk-management measures for essential and important entities that could entail supply chain security measures that require the use of products with digital elements meeting stricter cybersecurity requirements than those laid down by this Regulation. In line with Directive (EU) 2022/2555 and its minimum harmonisation principle, Member States may therefore impose additional or stricter cybersecurity requirements for the use of ICT products by essential or important entities under the scope of 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 manufacturers thereof. Member States may therefore lay down national measures, including restrictions on products with digital elements or suppliers of such products ~~from national markets~~, that take account of non-technical factors. National measures relating to such factors must comply with Union law.

(New recital corresponding to Art 4, para ~~3b~~5):

This Regulation should be without prejudice to the Member States' prerogatives to take measures safeguarding national security, in compliance with Union law. Member States should be able to subject products with digital elements that will be used for military, defence or national security purposes, to additional measures.

(New recital):

The obligations laid down in this Regulation should not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' security.

(9a) The definition of products with digital elements also includes remote data processing solutions to ensure 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. The processing or storage at a distance is covered only in so far as necessary for a products with digital elements to perform its functions. This could for instance be the case where a hardware device requires access to an application programming interface or a database developed by the

manufacturer. The requirements concerning the remote data processing solutions under the scope of this Regulation do not therefore entail technical, operational and organisational measures aimed at managing the risks posed to the security of their network and information systems as a whole.

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

This Regulation applies only 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. The supply in the course of a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by 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. The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity. Hosting of open-source software in code or binary form, participation in open-source projects and support for open-source solutions, does neither make the person, its organization nor the OSS project a manufacturer.

Taking account of the above-mentioned elements determining the commercial nature of an activity, only free and open-source software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable, should not be covered by this Regulation. The manufacturer of a commercial product with digital elements becomes the manufacturer of all open-source components in the supplied product and only for the scope of the supplied product. Commercial activity does not include the mere availability of open-source software to the public. Donations, membership fees, and financial sponsorships received by non-profit open-source organisations and other repositories do not constitute a commercial activity either, nor do revenues generated from ancillary services, such as technical support, when provided by non-profit organisations.

(11) A secure Internet is indispensable for the functioning of critical infrastructures and for society as a whole. ~~[~~Directive **(EU) 2022/2555**~~XXX/XXXX (NIS2)]~~ aims at ensuring a high level of cybersecurity of services provided by essential and important entities, including digital infrastructure providers that support core functions of the open Internet, ensure Internet access and Internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the

Internet are developed in a secure manner and that they comply with well-established Internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under ~~the [~~Directive **(EU) 2022/2555~~XXX/XXXX (NIS2)]~~** by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products.

(11a) 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 create processes to ensure that internet-connected products with digital elements include functions that enable the notification, distribution and installation of security updates automatically. They should also provide the possibility to approve the installation of the security updates as a final step, as well as clear instructions on how users can opt out of automatic updates. The requirements relating to automatic updates laid down in Annex I of this Regulation are not applicable to products primarily intended to be integrated as components into other products. They also do not apply to products for which users would not reasonably expect automatic updates, including in critical environments where an automatic update could cause interference with operations, such as in industrial environments.

(12) Regulation (EU) 2017/745 of the European Parliament and of the Council[1] lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council[2] lays down rules on *in vitro* diagnostic medical devices. Both Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole life cycle approach are also covered by those Regulations. These requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including *in vitro* diagnostic devices, with guidance on how to fulfil all the relevant essential requirements of Annex I to those Regulations with regard to cybersecurity.[3] Products with digital elements to which either of those Regulations apply should therefore not be subject to this Regulation.

---

[1] 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).

[2] 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).

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

(13) Regulation (EU) 2019/2144 of the European Parliament and of the Council[4][5][6] establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire lifecycle of vehicles, equipment and services in compliance with the applicable United Nations regulations on technical specifications and cybersecurity[7], and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council[8] is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats. Products with digital elements to which Regulation (EU) 2019/2144 applies and those products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation., The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation.

(14) This Regulation lays down horizontal cybersecurity rules which are not specific to sectors or certain products with digital elements. Nevertheless, sectoral or product-specific Union rules could be introduced, laying down requirements that address all or some of the risks covered by the essential requirements laid down by this Regulation. In such cases, the application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I of this Regulation may be limited or excluded where such limitation or exclusion is consistent with the overall regulatory framework applying to those products and

where the sectoral rules achieve at least the same level of protection as the one provided for by this Regulation. The Commission is empowered to adopt implementing acts to amend

---

[4] 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 [5] /2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No [6] /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).*

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

[8] 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).

this Regulation by identifying such products and rules. For existing Union legislation where such limitations or exclusions should apply, this Regulation contains specific provisions to clarify its relation with that Union legislation.

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

(16) Directive 85/374/EEC[9] is complementary to this Regulation. That Directive sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault ('strict liability'). Where such a lack of safety consists in a lack of security updates after placing the product on the market, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such security updates should be laid down in this Regulation.

(17) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council[10], including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data

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

[10] 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).

Protection Board (EDPB) established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and the Union data protection law should also be created in the area of market surveillance and enforcement. To this end, national market surveillance authorities appointed under this Regulation should cooperate with authorities supervising Union data protection law. The latter should also have access to information relevant for accomplishing their tasks.

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

(18a) When integrating components sourced from third parties in products with digital elements, manufacturers should exercise due diligence. The appropriate level of due diligence measures should be informed by the nature and level of the cybersecurity risk associated with the component and, for this purpose, take into account specific factors, such as the way in which the component contributes to the functionality of the product and the extent to which it has access to data processed by the product with digital elements. Depending on the risk, due diligence measures could include: verifying that the manufacturer of a component has demonstrated conformity with this Regulation, verifying that a component is free from vulnerabilities registered in publicly accessible vulnerability databases, or verifying that a component receives regular security updates.

(19) ~~Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it gathers,~~ ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group ~~referred to in~~ **established under** Directive **(EU) 2022/2555** ~~[Directive XXX / XXXX (NIS2)]~~. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be conducted by market

surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised. In exceptional circumstances, at the request of the Commission, ENISA should be able to ~~conduct~~ **provide an analysis to support an** evaluation**s** in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market. **[Entire recital to be re-evaluated in light of ENISA's role discussions]**

(19a) **[New recital regarding actively exploited vulnerabilities to be drafted based on further discussions/or workshops].**

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

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

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

(22a) Where security updates, which are designed to decrease the level of risk of a product with digital elements, do not modify the original intended functions, type or performance of a product, they are not considered a substantial modification. For example, this could be the case where a security update addresses a known vulnerability. Where feature updates modify the original intended functions or the type or performance of a product, they should be considered a substantial modification, as the addition of new features typically leads to a broader attack

surface, thereby increasing the 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. It should also be considered a significant modification when software updates combine both security and feature updates.

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

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

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

(26) ~~**Critical**~~ **Certain categories of** products with digital elements should be subject to stricter conformity assessment procedures, while keeping a proportionate approach. For this purpose, ~~**critical**~~ **those categories of** products with digital elements should be divided into two classes, reflecting the level of cybersecurity risk linked to these categories of products. **The categories of products with digital elements listed in class I of Annex III either have a cybersecurity-related functionality or perform a central system function, whereas those listed in class II of Annex III meet both these criteria. Cumulating these criteria indicates that** a potential cyber incident involving products in class II might lead to greater negative impacts than an incident involving products in class I, ~~**for instance**~~ due to the nature of their cybersecurity-related function **and the performance of a central sytem function** ~~**or intended use in sensitive environments**~~, and therefore should undergo a stricter conformity assessment procedure.

(27) The categories of ~~**critical**~~ products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation

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

(27a) In order to ensure a common adequate cybersecurity protection of highly critical products with digital elements in the Union, the Commission should be empowered to adopt implementing acts which supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers are 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 category of products with digital elements can be considered highly critical if there is a high critical dependency by entities of a type referred to in Annex I to Directive (EU) 2022/2555 or, if affected by cybersecurity incidents or when containing exploited vulnerabilities, can lead to serious disruptions for critical supply chains. When assessing the need for specifying categories of highly critical products with digital elements by means of a delegated act, the Commission may take into account whether the Member States identified at national level products with digital elements that have a critical role for the resilience of entities of a type referred to in Annex I to Directive (EU) 2022/2555 and which increasingly face supply chain cyber attacks, with potential serious disruptive effects.

(28) This Regulation addresses cybersecurity risks in a targeted manner. Products with digital elements might, however, pose other safety risks, that are not related to cybersecurity. Those risks should continue to be regulated by other relevant Union product legislation. If no other Union harmonisation legislation is applicable, they should be subject to Regulation [General Product Safety Regulation]. Therefore, in light of the targeted nature of this Regulation, as a derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] should apply to products with digital elements with respect to safety risks not covered by this Regulation, if those products are not subject to specific requirements imposed by other Union harmonisation legislation within the meaning of [Article 3, point (25) of the General Product Safety Regulation].

(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation[11] [the AI Regulation] which fall within the scope of this Regulation should comply with the essential requirements set out in this Regulation. When those high-risk AI systems fulfil the essential requirements of this Regulation, they should be deemed compliant with the cybersecurity requirements set out in Article [Article 15] of Regulation [the AI Regulation] in so far as those requirements are covered by the EU declaration of conformity or parts thereof issued under this Regulation. As regards the conformity assessment procedures relating to the essential cybersecurity requirements of a product with digital elements covered by this Regulation and classified as a high-risk AI system, the relevant provisions of Article 43 of Regulation [the AI Regulation] should apply as a rule instead of the respective provisions of this Regulation. However, this rule should not result

[11] Regulation [the AI Regulation].

in reducing the necessary level of assurance for critical products with digital elements covered by this Regulation. Therefore, by way of derogation from this rule, high-risk AI systems that fall within the scope of the Regulation [the AI Regulation] and are also **~~qualified as critical~~** products with digital elements **as referred to in Annex III,** pursuant to this Regulation and to which the conformity assessment procedure based on internal control referred to in Annex VI of the Regulation [the AI Regulation] applies, should be subject to the conformity assessment provisions of this Regulation in so far as the essential requirements of this Regulation are concerned. In this case, for all the other aspects covered by Regulation [the AI Regulation] the respective provisions on conformity assessment based on internal control set out in Annex VI to Regulation [the AI Regulation] should apply.

(30) **To the extent that ~~The machinery~~** products falling within the scope of Regulation [Machinery Regulation proposal] **are products with digital elements within the meaning of this Regulation, manufacturers of these products should comply with both the essential requirements established by this Regulation and ~~which are products with digital elements within the meaning of this Regulation and for which a declaration of conformity has been issued on the basis of this Regulation should be deemed to be in conformity with~~** the essential health and safety requirements set out in **the Regulation [Machinery Regulation proposal]. The essential requirements under this Regulation and certain essential requirements of the [Machinery Regulation proposal] might address similar aspects. For instance, compliance with the essential requirements under this Regulation could facilitate the compliance with the essential requirements related to cybersecurity regarding the protection against corruption and safety and reliability of control systems set out in** [Annex III, sections 1.1.9 and 1.2.1] of the Regulation [Machinery Regulation proposal]**~~, as regards protection against corruption and safety and reliability of control systems in so far as the compliance with those requirements is demonstrated by the EU declaration of conformity issued under this Regulation~~**. **A manufacturer may identify such synergies during the risk assessment process as foreseen under the [Machinery Regulation proposal]. Furthermore, 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 the [Machinery Regulation proposal] 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 Regulation [Machinery Regulation proposal].**

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

(32) In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as throughout their life-cycle, it is necessary to lay down essential requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential requirements related to vulnerability handling and ensure that all their products are delivered without any known exploitable vulnerabilities, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product. For this purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential requirements and in order to appropriately apply suitable harmonised standards or common specifications.

(32a) Where certain essential 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 requirement would be incompatible with the nature of a product with digital elements. For example, the intended purpose of a product may require the manufacturer to follow widely recognised interoperability standards even if their security features are no longer considered state of the art. Similarly, other Union legislation may require manufacturers to apply specific interoperability requirements. This is for example the case of Commission Implementing Regulation (EU) 2019/838 on technical specifications for vessel tracking and tracing systems and repealing Regulation (EC) No 415/2007, which specifies how AIS transponders should communicate with one another.

(33) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential requirements. These essential requirements should be without prejudice to the ~~EU~~ **Union level** coordinated **security** risk assessments of critical supply chains established **pursuant to~~by~~ [**Article **22~~X~~]** of Directive **(EU) 2022/2555~~[Directive XXX/XXXX(NIS2)]~~**[12], which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, it should be without prejudice to the Member States' prerogatives to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Recommendation (EU) 2019/534, in the ~~Union-wide~~**EU** coordinated risk assessment of **the cybersecurity of** 5G networks ~~security~~ and in the EU Toolbox on 5G cybersecurity agreed by the ~~NIS~~ Cooperation Group ~~as referred to in~~ **[established under** Directive **(EU) 2022/2555~~XXX/XXXX (NIS2)~~]**.

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

~~[12] Directive XXX of the European Parliament and of the Council of [date] [on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ L xx, date, p.x)].~~

European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database.]

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

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

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

(38) In order to facilitate assessment of conformity with the requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements which are in conformity with harmonised standards, which translate the essential requirements of this Regulation into detailed technical specifications, and which are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council[19]. Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements of this Regulation.

(39) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, processes and services. European cybersecurity certification

[19] 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).

schemes can cover products with digital elements covered by this Regulation. This Regulation should create synergies with Regulation (EU) 2019/881. In order to facilitate the assessment of conformity with the requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and which has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity certification schemes for products with digital elements should be assessed in the light of this Regulation. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation. The Commission should be empowered to specify, by means of implementing acts, the European cybersecurity certification schemes that can be used to demonstrate conformity with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, where applicable, the Commission should specify if a cybersecurity certificate issued under such European cybersecurity certification schemes eliminates the obligation for manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements.

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

(41) **The current EU 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 requirements of 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, w~~W~~**here no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of

this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation request by any of the European standardisation organisations, undue delays in the establishment of appropriate harmonised standards, or a lack of compliance of developed standards with the requirements of this Regulation or with a request of the Commission. **If a delay is due to the technical complexity of the standard in question, this should be considered by the Commission before contemplating the establishment of common specifications.**

(41a) With a view to establishing, in the most efficient way, common specifications that cover the essential requirements of this Regulation, the Commission should involve relevant stakeholders in the process.

(41b) Reasonable period should mean, in relation to the publication of reference to harmonised standards in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012, 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.

(41c) In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.

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

(43) The CE marking, indicating the conformity of a product, is the visible consequence of a whole process comprising conformity assessment in a broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council[13]. Rules governing the affixing of the CE marking on products with digital elements should be laid down in this Regulation. The CE marking should be the only marking which guarantees that products with digital elements comply with the requirements of this Regulation.

(44) In order to allow economic operators to demonstrate conformity with the essential requirements laid down in this Regulation and to allow market surveillance authorities to

[13] 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).

ensure that products with digital elements made available on the market comply with these requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council[14] establishes modules for conformity assessment procedures in proportion to the level of risk involved and the level of security required. In order to ensure inter-sectoral coherence and to avoid ad-hoc variants, conformity assessment procedures adequate for verifying the conformity of products with digital elements with the essential requirements set out in this Regulation have been based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole life cycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product.

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

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

[14] 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).

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

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

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

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

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

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

(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.

(54) Market surveillance is an essential instrument in ensuring the proper and uniform application of Union legislation. It is therefore appropriate to put in place a legal framework within which market surveillance can be carried out in an appropriate manner. Rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 of the European Parliament and of the Council[15] apply to products with digital elements covered by this Regulation.

(55) In accordance with Regulation (EU) 2019/1020, market surveillance authorities carry out market surveillance in the territory of that Member State. This Regulation should not prevent Member States from choosing the competent authorities to carry out those tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States may choose to designate any existing or new authority to act as market surveillance authority, including **~~national~~** competent authorities **~~referred to in established pursuant to~~** Article **8** **~~[Article X]~~** of **~~Directive [~~**Directive **(EU) 2022/2555~~~~XXX/XXXX (NIS2)]~~** or designated national cybersecurity certification authorities referred to in Article 58 of Regulation (EU) 2019/881. Economic operators should fully cooperate with market surveillance authorities and other competent authorities. Each Member State should inform the Commission and the other Member States of its market surveillance authorities and the areas of competence of each of those authorities and should ensure the necessary resources and skills to carry out the surveillance tasks relating to this Regulation. As per Article 10(2) and (3) of Regulation (EU) 2019/1020, each Member State should appoint a single liaison office that should be responsible, among others, for representing the coordinated position of the market surveillance authorities and assisting in the cooperation between market surveillance authorities in different Member States.

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

(57) In order to ensure timely, proportionate and effective measures in relation to products with digital elements presenting a significant cybersecurity risk, a Union safeguard procedure should be foreseen under which interested parties are informed of measures intended to be taken with regard to such products. This should also allow market surveillance authorities, in cooperation with the relevant economic operators, to act at an earlier stage where necessary. Where the Member States and the Commission agree as to the justification of a measure taken by a Member State, no further involvement of the Commission should be

[15] 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).

required, except where non-compliance can be attributed to shortcomings of a harmonised standard.

(58) In certain cases, a product with digital elements which complies with this Regulation, may nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by **~~essential~~** entities of **a ~~the~~** type referred to in **~~[~~**Annex I to Directive **(EU) 2022/2555~~XXX/XXXX (NIS2)]~~** or to other aspects of public interest protection. Therefore it is necessary to establish rules which ensure mitigation of those risks. As a result, market surveillance authorities should take measures to require the economic operator to ensure that the product no longer presents that risk, to recall it or to withdraw it, depending on the risk. As soon as a market surveillance authority restricts or forbids the free movement of a product in such way, the Member State should notify without delay the Commission and the other Member States of the provisional measures, indicating the reasons and justification for the decision. Where a market surveillance authority adopts such measures against products presenting a risk, the Commission should enter into consultation with the Member States and the relevant economic operator or operators without delay and should evaluate the national measure. On the basis of the results of this evaluation, the Commission should decide whether the national measure is justified or not. The Commission should address its decision to all Member States and immediately communicate it to them and the relevant economic operator or operators. If the measure is considered justified, the Commission may also consider adopting proposals to revise the respective Union legislation.

(59) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that these are not compliant with this Regulation, or for products that are compliant with this Regulation, but that present other important risks, such as risks to the health or safety of persons, fundamental rights or the provision of the services by **~~essential~~** entities of **~~a~~the** type referred to in **~~[~~**Annex I **~~to~~of** Directive **(EU) 2022/2555~~XXX / XXXX (NIS2)]~~**, the Commission may request ENISA to carry out an evaluation. Based on that evaluation, the Commission may adopt, through implementing acts, corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling of the respective products, within a reasonable period, commensurate with the nature of the risk. The Commission may have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the good functioning of the internal market, and only where no effective measures have been taken by surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities under the scope of **~~[~~**Directive **(EU) 2022/2555~~XXX / XXXX (NIS2)]~~**, while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the noncompliance with this Regulation or the important risks presented persist.

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

(61) Simultaneous coordinated control actions ('sweeps') are specific enforcement actions by market surveillance authorities that can further enhance product security. Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA

should submit proposals for categories of products for which sweeps could be organised to the market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives.

(62) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission in respect of updates to the list of ~~**critical**~~ products in Annex III and specifying the definitions of the these product categories. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential mandating of certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[16]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to: specify the format and elements of the software bill of materials, specify further the type of information, format and procedure of the notifications on actively exploited vulnerabilities and incidents submitted to ENISA by the manufacturers, specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts therefore as set out in Annex I of this Regulation, adopt common specifications in respect of the essential requirements set out in Annex I, lay down technical specifications for pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use, decide on corrective or restrictive measures at Union level in exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[17].

---

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

[17] 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).

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

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

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

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

(new recital:)

Consumers should be entitled to enforce their rights in relation to the obligations imposed on economic operators under this Regulation through representative actions in accordance with Directive (EU) 2020/1828 of the European Parliament and of the

Council[18]. 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 that amendment is reflected in their transposition measures adopted in accordance with 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 against infringements by economic operators of provisions of this Regulation that harm or can harm the collective interests of consumers should start from the date of application of this Regulation.

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

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

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

(71) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[19] and delivered its opinion on […],

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

[18] **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).**

[19] 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).

This Regulation lays down:

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

(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;

(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;

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

Article 2

Scope

1. This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.
2. Regulation does not apply to products with digital elements to which the following Union acts apply:

   (a) Regulation (EU) 2017/745;

   (b) Regulation (EU) 2017/746;

   (c) Regulation (EU) 2019/2144.

3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.
4. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:

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

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

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

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

Article 3

Definitions

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

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

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

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

4) **~~'highly critical product with digital elements' means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(5);~~**[20]

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

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

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

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

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

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

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

[20] **Defintion not necessary since highly critical is defined in Article 6a and in recitals.**

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

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

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

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

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

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

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

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

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

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

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

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

(24) ‘intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in

the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

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

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

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

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

(29) 'conformity assessment body' means a **conformity assessment** body **as** defined in Article 2**, point** (13)**,** of Regulation (EU) No 765/2008;

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

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

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

(33) 'market surveillance authority' means ~~the~~ **a market surveillance** authority as defined in Article 3, point (4)**,** of Regulation (EU) 2019/1020;

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

(35) 'cybersecurity risk' means risk as defined in Article **2,point (9),**~~**[Article X]**~~ of Directive **(EU) 2022/2555**~~**[Directive XXX/XXXX (NIS2)]**~~;

(36) 'significant cybersecurity risk' means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead

to a severe negative impact, including by causing considerable material or non-material loss or disruption;

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

(38) 'vulnerability' means a vulnerability as defined in Article **2, point (15),** [~~**Article X**~~] of Directive **(EU) 2022/2555** [~~**Directive XXX/XXXX (NIS2)**~~];

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

(40) 'personal data' means **personal** data as defined in Article 4**, point** (1)**,** of Regulation (EU) 2016/679.

(xx) 'recall' means recall as defined in Article 3, point (22), of Regulation (EU) 2019/1020;

(xx) 'withdrawal' means withdrawal as defined in Article 3, point (23), of Regulation (EU) 2019/1020.

(xx) 'incident having an impact on the security of the product with digital elements' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555 which negatively affects the ability of a manufacturer's product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions.

(xx) 'micro, small and medium-sized enterprises' or 'SMEs' means micro, small and medium-sized enterprises as defined in the Annex to Recommendation 2003/361/EC;

(xx) 'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881.

Article 4

Free movement

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

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

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

4. **Paragraph 3 does not apply to safety components as specified under other Union harmonisation legislation.**

5. **This Regulation shall not prevent Member States from subjecting products with digital elements and their economic operators to additional measures when these products are intended to or will be used for military, defence or national security purposes, and such measures are necessary and proportionate for the achievement of those purposes. The same applies to additional or deviating measures when such measures are proportionate for safeguarding products, infrastructures or processed information and these specific products will be used:**

   (a) **for critical system functions or critical components deployed in sectors of high criticality as defined in XXX (Annex I, NIS2 directive).**

   (b) **in EHR systems as defined in XXX (COM/2022/197 final); or**

   (c) **in smart metering systems as defined in DIRECTIVE (EU) 2019/944 that are used to control consumption or generation of electricity in the smart grid; o**

   (d) **in products and corresponding infrastructures for preventing tax fraud; or**

   (e) **in electronic identification schemes as defined in Article 3(4) of Regulation (EU) 910/2014 that are provided or to be notified by the Member State; or**

   (f) **for trust services as defined in Article 3(16) of Regulation (EU) 910/2014 that are provided by the Member State; or**

   (g) **for European Digital Identity Wallets as defined in Article 3(42) of Regulation (EU) XXX that are provided by the Member State, under a mandate from the Member State or independently of a Member State but to be recognised by the Member State; or**

   (h) **in trust and background infrastructures supporting functions, components, systems, entities, schemes, identification means and infrastructures described in point (a) to (h).**

6.

Article 5

Requirements for products with digital elements

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

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

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

Article 6

Critical Classification of products with digital elements subject to specific conformity assessment procedures ~~and highly critical products with digital elements~~

1. **~~Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements~~**. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall **be subject to the conformity assessment procedures referred to in Article 24 (2) and (3). ~~be considered as falling in belonging to that category.~~**

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

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

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

   The categories of products with digital elements listed in class II of Annex III meet ~~at least two of~~ both ~~the following~~ criteria referred to in points (a) and (b) of this paragraph,~~:~~.

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

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

   ~~(c) the intended use application of the product with digital elements in sensitive environments[28], including in industrial control settings or and by essential entities of the a type referred to in the Annex I to the Directive (EU) 2022/2555 [Directive XXX:XXXX (NIS2)].~~

~~2.~~3. [The Commission is empowered to adopt implementing acts in accordance with Article 50 to amend Annex III by including in the list **within each class** of **the** categories of **~~critical~~** products with digital elements a new category or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the **~~level~~ function** of **~~cybersecurity risk related to the category of the~~** products with digital elements. **~~In determining the level of cybersecurity risk, one~~**

~~or~~ **several of the following criteria referred to in paragraph 1 of this Article shall be taken into account.:**

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

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

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

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

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

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

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

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

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

~~3.~~4. [The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by 12 months since the entry into force of this Regulation].]

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

Article 6a

Highly critical products with digital elements

~~5.~~ [The Commission is empowered to adopt implementing acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European

cybersecurity certificate **at assurance level 'high'** under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account **the criteria referred to in paragraph ~~1~~2 of ~~this~~ Article 6 ~~the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2,~~** as well as **~~in view of the assessment of whether that category of products is~~ any of the following criteria**:

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

(b) **~~relevant for the resilience of the overall~~ the extent to which cybersecurity incidents and exploited vulnerabilities concerning the category of products with digital elements can lead to disruptions to ~~disruptive events~~[21] ~~for~~ critical** supply chains ~~of products with digital elements against disruptive events~~ **across the internal market.]**

Article 7

General product safety

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

Article 8

High-risk AI systems

1. **Without prejudice to the requirements relating to accuracy and robustness set out in Article [Article 15]** ~~Products with digital elements classified as high-risk AI systems in accordance with Article [Article 6]~~ of Regulation [the AI Regulation]**, products with digital elements** which fall within the scope of this Regulation~~,~~ **and which are classified as high-risk AI systems pursuant to Article [Article 6] of Regulation [the AI Regulation]** ~~and fulfil the essential requirements set out in Section 1 of Annex I of this~~

[21] ~~**A recital may be added.**~~

~~Regulation, and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I,~~ shall be deemed ~~in~~ complian~~tee~~ with the **cybersecurity** requirements ~~related to cybersecurity~~ set out in Article [Article 15] of **that** Regulation ~~[the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.~~ **if:**

(a) they fulfil the essential requirements set out in Section 1 of Annex I to this Regulation;

(b) the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I to this Regulation; and

(c) the achievement of the level of cybersecurity protection required under Article [Article 15] of Regulation [the AI Regulation] 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, the relevant conformity assessment procedure as required by Article [Article 43] of Regulation [AI Regulation] shall apply. For the purpose of that assessment, notified bodies which are ~~entitled~~ **competent** to control the conformity of the high-risk AI systems under ~~the~~ Regulation [AI Regulation] shall be also ~~entitled~~ **competent** to control the conformity of ~~the~~ 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 29 of this Regulation ~~have~~

has been assessed in the context of the notification procedure under Regulation [AI Regulation].

3. By **way of** derogation from paragraph 2, critical products with digital elements listed in Annex III ~~of~~ **to** this Regulation, which ~~have to apply~~ **are subject to** the conformity assessment procedures referred to in Articles 24(2)(a), 24(2)(b), 24(3)(a) and 24(3)(b) ~~under~~ **of** this Regulation and which are also classified as high-risk AI systems ~~according~~**pursuant** to Article [Article 6] of ~~the~~ Regulation [AI Regulation]**,** and to which the conformity assessment procedure based on internal control referred to in Annex [Annex VI] to Regulation [the AI Regulation] applies, shall be subject to the conformity assessment procedures ~~as~~ required ~~by~~ **under** this Regulation in so far as the essential requirements of this Regulation are concerned.

~~***Article 9***~~

~~***Machinery products***~~

~~**Machinery products under the scope of Regulation [Machinery Regulation proposal] which are products with digital elements within the meaning of this Regulation and for which an EU declaration of conformity has been issued on the basis of this Regulation shall be deemed to be in conformity with the requirements related to**~~

~~**cybersecurity regarding the protection against corruption and safety and reliability of control systems essential health and safety requirements set out in Sections 1.1.9 and 1.2.1 of Annex [Annex III, Sections 1.1.9 and 1.2.1] to Regulation [Machinery Regulation proposal], as regards protection against corruption and safety and reliability of control systems, and in so far as if the achievement of the level of cybersecurity protection required by under those requirements Sections is demonstrated in the EU declaration of conformity issued under pursuant to this Regulation.**~~

CHAPTER II

OBLIGATIONS OF ECONOMIC OPERATORS

Article 10

Obligations of manufacturers

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

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

2a. The risk assessment referred to in paragraph 1 shall be documented and updated as appropriate during the expected lifetime of the product. It shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the specific conditions of use of the product with digital elements, such as the operational environment, and the assets to be protected, taking into account the whole lifecycle of the product. The risk assessment shall indicate the specific security requirements as set out in point 3 of section 1 of Annex I that are applicable to the respective product with digital elements and how these are implemented as informed by the risk assessment.

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

4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from

third parties ~~in products with digital elements~~ **in a manner that such components do not compromise the security of the product with digital elements.** ~~**They shall ensure that such components do not compromise the security of the product with digital elements.**~~

5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities ~~**they**~~ **it** becomes aware of and any relevant information provided by third parties, and, where applicable, update the **cybersecurity** risk assessment of the product.

6. ~~**When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter,**~~ **M**anufacturers shall ensure**, when placing a product with digital elements on the market** ~~**and for a period of time after the placing on the market appropriate to the type of**~~ and ~~**its**~~ **for the expected product lifetime**, that vulnerabilities of that product **and components not supplied in the course of a commercial activity integrated in it** are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

Manufacturers shall determine the expected product lifetime referred to in the first subparagraph of this paragraph taking into account the time users reasonably expect to be able to use the product given its functionality and intended purpose and therefore can expect to receive security updates.

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

Security updates, referred to in Section 2, point (8), of Annex I, which have been made available to users shall remain available for a minimum duration of 10 years.

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

They shall carry out the chosen conformity assessment procedures referred to in Article 24.

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

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

9. Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity **with the requirements of this Regulation**. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 1**89** by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.

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

10a. Manufacturers shall clearly and understandably specify in an easily accessible manner and where applicable on the packaging of the product with digital elements, the end date for the expected product lifetime as referred to in paragraph 6, including at least the month and year, until which the manufacturer will at least ensure the effective handling of vulnerabilities in accordance with the essential requirements set out in Section 2 of Annex I.

11. 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 be ~~or~~** include**d** in the instructions and information set out in Annex II the internet address at which the **full** EU declaration of conformity can be accessed.

12. From the placing on the market and for the **period of time referred to in paragraph 6 ~~expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter~~**, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.

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

cybersecurity risks posed by the product with digital elements, which they have placed on the market.

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

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

Article 11

Reporting obligations of manufacturers

1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify **to the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure ~~in accordance with~~ pursuant to Article ~~[Article X]~~ 12(1) of Directive ~~[Directive XXX/XXXX (NIS2)]~~(EU) 2022/2555 of Member States concerned [through a single reporting platform] ~~to ENISA~~** any actively exploited vulnerability contained in the product with digital elements. The notification shall include **technical** details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken.

~~ENISA~~ **The CSIRTs** shall, without undue delay, unless for ~~justified~~ cybersecurity risk-related grounds, forward the notification to **ENISA ~~the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt~~** and inform the market surveillance authorit**ies of all the concerned Member States** about the notified vulnerability.

2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify **~~to ENISA~~ the single point of contact designated or established ~~in accordance with~~ pursuant to Article ~~[Article X]~~8(3) of Directive (EU) 2022/2555 ~~[Directive XXX/XXXX (NIS2)]~~ of the Member States concerned [through a single reporting platform]** any incident having impact on the security of the product with digital elements. **~~ENISA~~ The ~~designated~~ single point of contact** shall, without undue delay, unless for ~~justified~~ cybersecurity risk-related grounds, forward the notifications to **~~the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned~~ ENISA** and inform the market surveillance authorit**ies in all concerned Member States** about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate

whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

2a. For all products with digital elements, the manufacturer shall have the possibility for the voluntary reporting of vulnerabilities of which active exploitation have not yet been observed.

2b. In the case that a third party other than manufacturer discloses an actively exploited vulnerability or an incident of a product under the scope of this Regulation to the CSIRT, the CSIRT shall without undue delay inform the manufacturer.

3. **The EU CSIRT-Network** ~~ENISA~~ shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established **~~by~~under** Article ~~[Article X]~~**16** of Directive **(EU) 2022/2555** ~~[Directive XXX/XXXX (NIS2)]~~ information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large- scale cybersecurity incidents and crises at an operational level.

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident in a standardized, structured and easily automatically processible machine-readable format.

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

6. ENISA, on the basis of the notifications received pursuant to paragraphs 1 and 2, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group **~~referred to~~ ~~in~~ established under** Article ~~[Article X]~~ **14** of Directive **(EU) 2022/2555**~~[Directive XXX/XXXX (NIS2)]~~. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.

7. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component. **Where manufacturers have developed a software modification to address the vulnerability in that component, they shall share the relevant code with the person or entity maintaining the component.**

Article 12

Authorised representatives

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

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

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

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

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

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

Article 13

Obligations of importers

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

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

(a) the appropriate conformity assessment procedures referred to in Article 24

have been carried out by the manufacturer;

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

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

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

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

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

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

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

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

8. Importers shall, further to a reasoned request from a competent nationalauthority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.

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

and to the extent possible, the users of the products with digital elements placed on the market.

Article 14

Obligations of distributors

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

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

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

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

3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform **without undue delay** the manufacturer and the market surveillance authorities to that effect.

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

   Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the national competent 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 nonconformity and of any corrective measures taken.

5. Distributors shall, further to a reasoned request from a national competent authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the

cybersecurity risks posed by a product with digital elements, which they have made available on the market.

6. When the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform, **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 15

Cases in which obligations of manufacturers apply to importers and distributors

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

Article 16

Other cases in which obligations of manufacturers apply

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

That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7),

Article 17

Identification of economic operators

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

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

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

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

Article 18

Presumption of conformity

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

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

2. The Commission shall, as provided in Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the essential requirements set out in Annex I.

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

Those implementing acts shall only be adopted 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 requirements set out in Annex I and:

(i) the request has not been accepted; or

(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 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 51(2).

4. **Before preparing the draft implementing act referred to in paragraph 3, 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 3 have been fulfilled.**

5. **When preparing the draft implementing act referred to in paragraph 3, the Commission shall take into account the views of relevant bodies or the expert group and shall duly consult all relevant stakeholders.**

6. 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 3, or parts thereof,** shall be presumed to be in conformity with the essential requirements set out in Annex I **covered by** those **common specifications or parts thereof.**

7. **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 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 3, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.**

8. **When a Member State considers that a common specification does not entirely satisfy the essential 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.**

~~3~~**9**. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate **at assurance level "substantial" or "high"** has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 and specified as per paragraph ~~4~~ **4**–**10**, shall be presumed to be in conformity with the essential requirements set out in Annex I **and related conformity assessment procedures** ~~in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements at the relevant assurance levels~~**.**

~~4~~ **4**–**10**. The Commission is empowered, by means of implementing acts, to specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I. ~~Furthermore, where applicable, the Commission shall specify if for which assurance levels, a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b). Those~~

~~implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).~~

~~*Article 19*~~

~~*[Common specifications][22] Presumption of conformity of products within the scope of this Regulation*~~

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

Article 20

EU declaration of conformity

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

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

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

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

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

~~[22] Will be updated according to Art 17 in the Machinery Regulation once it is finalised.~~

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

Article 21

General principles of the CE marking

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

Article 22

Rules and conditions for affixing the CE marking

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

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

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

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

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

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

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

Article 23

Technical documentation

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

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

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

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

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

Article 24

Conformity assessment procedures for products with digital elements

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

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

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

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

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

2. Where, in assessing the compliance of the ~~**critical**~~ product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer ~~**or the manufacturer's authorised representative**~~ has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18,

or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to ~~either~~ **any** of the following procedures:

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

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

(c) **where applicable, a European cybersecurity certification scheme as specified in Article 18(~~3~~ 9) and (~~4~~ 10) at assurance level 'substantial' or 'high'.**

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

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

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

(c) **where applicable, a European cybersecurity certification scheme as specified in Article 18 (~~3~~ 9) and (~~4~~ 10) at assurance level 'substantial' or 'high'.**

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

5. ~~Notified bodies shall take into account the specific interests and needs of small and medium sized enterprises (SMEs) when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs.~~ **The specific interests and needs of SMEs[23], including start-ups, shall be taken into account when setting the fees for conformity assessment, reducing those fees proportionately to their size, market size and other relevant indicators.**

CHAPTER IV

NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

[23] A definition ~~will~~ **has been** added.

Article 25

Notification

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

Article 26

Notifying authorities

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

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

3. **Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 to a body which is not a governmental entity, that body shall be a legal entity and shall comply mutatis mutandis with the requirements laid down in [Article 27] of this Regulation. In addition it shall have arrangements to cover liabilities arising out of its activities.**

4. **The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3.**

Article 27

Requirements relating to notifying authorities

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

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

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

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

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

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

Article 28

Information obligation on notifying authorities

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

2. The Commission shall make that information publicly available.

Article 29

Requirements relating to notified bodies

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

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

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

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

4. A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, **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 those products, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services.

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

5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and

inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.

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

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

(a) ~~staff~~ **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 carried out, ensuring the transparency and the ability of reproduction of those procedures. It shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities;

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

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

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

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

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

(c) appropriate knowledge and understanding of the essential requirements **set out in Annex I**, of the applicable harmonised standards as well as the common

specifications and of the relevant provisions of

Union harmonisation legislation and of its implementing acts;

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

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

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

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

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

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

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

Article 30

Presumption of conformity of notified bodies

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

Article 31

Subsidiaries of and subcontracting by notified bodies

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

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

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

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

Article 32

Application for notification

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

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

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

Article 33

Notification procedure

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

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

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

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

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

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

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

Article 34

Identification numbers and lists of notified bodies

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

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

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

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

Article 35

Changes to notifications

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

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

Article 36

Challenge of the competence of notified bodies

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

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

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

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

Article 37

Operational obligations of notified bodies

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

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

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

4. Where a notified body finds that requirements laid down in Annex I or in corresponding harmonised standards or in common specifications as referred to in Article 1**98** have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a ~~conformity~~ 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 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 X

Appeal against decisions of notified bodies

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

Article 38

Information obligation on notified bodies

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

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

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

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

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

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

Article 39

Exchange of experience

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

Article 40

Coordination of notified bodies

1. The Commission shall ensure that appropriate coordination and cooperation between notified bodies are put in place and properly operated in the form of a cross-sectoral group of notified bodies.

2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

CHAPTER V

MARKET SURVEILLANCE AND ENFORCEMENT

Article 41

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

1. Regulation (EU) 2019/1020 shall apply to the products with digital elements within the scope of this Regulation.

2. Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation.

3. Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated under Article 58 of Regulation (EU) 2019/881 and exchange information on a regular basis. With respect to the supervision of

the implementation of the reporting obligations pursuant to Article 11 of this Regulation, the designated market surveillance authorities shall cooperate with ENISA.

4. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, and exchange information on a regular basis.

5. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing these authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 8 of this Article if such guidance and advice concerns the processing of personal data.

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

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

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

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

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

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

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

Article 42

Access to data and documentation

Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data, **in electronic form and 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 respective economic operator.

Article 43

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

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

   Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant **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 risk, as ~~it~~ **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 ~~appropriate~~ corrective actions.

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

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

4. Where the ~~manufacturer~~ **economic operator** ~~of a product with digital elements~~ does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph, the market surveillance authority shall take ~~all~~ appropriate provisional

measures to prohibit or restrict that product **with digital elements from** being made available on its national market, to withdraw it from that market or to recall it.

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

5. The information referred to in paragraph 4 shall include all available details, in particular the data necessary for the identification of the non-compliant products with digital elements, the origin of ~~the~~ **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 requirements set out in Annex I;

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

6. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product **with digital elements** concerned, and, in the event of disagreement with the notified national measure, of their objections.

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

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

Article 44

Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 43(4), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union ~~legislation~~**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 43(4) and notify ~~such~~ **that** decision to the Member State concerned.

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

3. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in the harmonised standards, the Commission shall apply the procedure provided for in Article ~~10~~ **11** of Regulation (EU) No 1025/2012.

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

5. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in common specifications as referred to in Article 1**98**, the Commission shall consider whether to amend or repeal the implementing act referred to in Article 1**98** setting out those common specifications.

Article 45

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

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

2. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product **with digital elements** referred to in paragraph 1 remains noncompliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission may request ENISA to **provide an analysis to support** ~~carry out~~ an evaluation of compliance.

   The Commission shall inform the relevant market surveillance authorities accordingly.

   The relevant economic operators shall cooperate as necessary with ENISA.

3. Based on ~~ENISA's~~**the** evaluation **referred to in paragraph 2**, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.

4. On the basis of the consultation referred to in paragraph 3, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal **of the product with digital elements** from the market, or recalling **of it**, within a reasonable period, commensurate with the nature of the risk. Those

implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

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

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

Article 46

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 appropriate measures where, having performed an evaluation under Article 43, 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 entities of a type referred to in Annex I to 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.

~~1. Where, having performed an evaluation under Article 43, the market surveillance authority of a Member State finds that although a product with digital elements and the processes put in place by the manufacturer are in compliance with this Regulation, they present a significant cybersecurity risk and, in addition, they pose a risk to the health or safety of persons, to the compliance with obligations under Union or national law intended to protect fundamental rights, the availability authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in [Annex I to Directive XXX / XXXX (NIS2)] or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that the product with digital elements and the processes put in place by the manufacturer concerned, when placed on the market, no longer present that risk, to withdraw the product with digital elements from the market or to recall it within a reasonable period, commensurate with the nature of the risk.~~

~~2.~~ The manufacturer or other relevant **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**s** involved and the nature and duration of the national measures taken.

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

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

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

~~7.~~ In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product **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 may request ENISA to **provide an analysis to support**~~carry out~~ an evaluation of the risks presented by that product **with digital elements** and shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

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

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

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

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

Article 47

Formal non-compliance

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

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

   (b) the ~~conformity~~ **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 48

Joint activities of market surveillance authorities

1. Market surveillance authorities may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed **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 may propose joint activities for checking compliance with this Regulation ~~**to be conducted by market surveillance authorities**~~ based on indications or information of potential non-compliance across several Member States of products **with digital elements** falling in the scope of this Regulation with the requirements laid down ~~by the latter~~**herein**.

3. The market surveillance authorities and**, where applicable,** the Commission, ~~where applicable,~~ shall ensure that the agreement to carry out joint activities does not lead to

unfair competition between economic operators and does not negatively affect the objectivity, independence and impartiality of the parties to the agreement.

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

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

Article 49

Sweeps

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

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

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

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

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

CHAPTER VI

DELEGATED POWERS AND COMMITTEE PROCEDURE

Article 50

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) shall be conferred on the Commission **for an indeterminate period of time from … [date of entry into force of this Regulation].**

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

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

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

6. A delegated act adopted pursuant to Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 51

Committee procedure

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

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

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

CHAPTER VII

CONFIDENTIALITY AND PENALTIES

Article 52

Confidentiality

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

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

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

(c) public and national security interests;

(d) integrity of criminal or administrative proceedings.

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

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law of the Member States.

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

Article 53

Penalties

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

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

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

4. The non-compliance with ~~any other~~ **the** obligations **set out in Articles [Articles12; 13; 14; 15; 16; 17; 20; 22 (1)-(4); 23 (1)-(4); 24(1)-(3); 29; 31; 37; 38; 42]** under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the

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

offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

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

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

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

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

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

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

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

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

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

CHAPTER VIII

TRANSITIONAL AND FINAL PROVISIONS

Article 54

Amendment to Regulation (EU) 2019/1020

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

’71. [Regulation XXX][Cyber Resilience Act]’.

Article XXX

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.

Article XXX

Amendment to Directive (EU) 2020/1828

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

'(XX) [Regulation XXX][Cyber Resilience Act]'

Article 55

Transitional provisions

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

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

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

Article 56

Evaluation and review

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

Article 57

Entry into force and application

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

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

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

Done at Brussels,

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

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

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

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

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

(aa) be placed on the market without any known vulnerabilities;

(a) be **placed on the market** ~~**delivered**~~ with a secure by default configuration, including the possibility to reset the product to its original **state, and including a default setting that security updates be installed automatically according to requirements in Annex I,2 (9) and Annex II,(8a), with a clear and easy- to-use opt-out mechanism.**

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

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

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

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

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

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

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

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

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

(k) ~~**ensure**~~ **enable** that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates **by default, but with a clear and easy-to-use opt-out mechanism, and where applicable through** the notification of available updates to users, **and the option to postpone them.**

(l) have a unique product identifier which allows the digital identification of the products . This unique product identifier is referenced in the security updates allowing an easy determination of the applicability of the patch.

(m) provide the possibility for users to securely and easily remove all data and settings (including those enabling access to specific networks) from the products and transfer the data safely to other products or systems to allow for a secure disposal of the product.

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

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

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

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, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and **clear and user friendly** information helping users to remediate the vulnerabilities where applicable and appropriate in a standardized, structured and easily automatically processable machine-readable format;

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 ~~**exploitable**~~ vulnerabilities are fixed or mitigated in a timely **and, where applicable, automatic** manner;

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

9) **where applicable under Annex I,1 (3)a, set as a default setting – which can be switched off – that security updates are installed automatically on products with digital elements if not installed within a certain timeframe;**

ANNEX II

INFORMATION AND INSTRUCTIONS TO THE USER

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

(1) the name, registered trade name or registered trade mark of the manufacturer, and the postal address ~~and the~~ email address **or other digital contact as well as**, **where applicable, the website** at which the manufacturer can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product;

(2) the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;

(3) the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;

(4) the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;

(5) any known or foreseeable circumstance, related to the use of the product **with** digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;

(6) ~~**if and, where applicable, where the software bill of materials can be accessed**~~;

(7) where applicable, **simplified EU declaration of conformity including** the internet address at which the **full** EU declaration of conformity can be **accessed**;

(8) the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates ~~.~~; **this earliest end date of support should also be clearly indicated at the time of purchase, in an easily accessible manner and where applicable on the product, its packaging and/or by digital means;**

(9) detailed instructions or an internet address referring to such detailed instructions and information on:

(a) the necessary measures during initial commissioning and throughout the **expected** lifetime of the product to ensure its secure use;

(b) how changes to the product can affect the security of data;

(c) how security-relevant updates can be installed;

(d) the secure decommissioning of the product, including information on how user data can be securely removed;

(e) **simple and clearly understandable instructions on how the default setting of automatically installed updates, as required by Annex I,2(9) can be turned off.**

(xx) If the manufacturer decides to make available the software bill of materials to the user, the information and instructions to the user accompanying the product with digital elements shall also include that software bill of materials as set out in Section 2, point (1) of Annex I.

ANNEX III

CLASSES AND CATEGORIES OF ~~CRITICAL~~ PRODUCTS WITH DIGITAL ELEMENTS

Class I

Categories of products with digital elements which meet the criteria referred to in Article 6(~~1~~ 2), ~~second subparagraph,~~ point (a):

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

~~2. Standalone and embedded browsers;~~

~~3. Password managers;~~

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

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

~~6. Network management systems;~~

~~7. Network configuration management tools;~~

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

~~9. Management of network resources;~~

~~2. 3. 10.~~ Security information and event management (SIEM) systems;

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

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

6. ~~3.~~ Public key infrastructure and digital certificate issu~~er~~sance software;

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

8. Wearable technology and other connected health devices;

9. Connected products intended for the use by and for children (including toys and baby monitors).

~~12. Application configuration management systems;~~

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

~~14. Mobile device management software;~~

~~15. Physical network interfaces;~~

Categories of products with digital elements which meet the criteria referred to in Article 6(~~1~~ 2), ~~second subparagraph,~~ point (b):

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

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

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

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

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

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

12a Remote desktop sharing software;

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

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

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

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

~~17. 20. Microcontrollers;~~

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

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

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

~~20.~~ ~~14.~~ ~~Robot sensing and actuator components and~~ Industrial robot controllers. 21. Microprocessors intended for integration in secure elements;

Class II

Categories of products with digital elements which meet both criteria referred to in Article 6(~~12~~), ~~third subparagraph,~~ points (a) and (b):

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

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

2. Authentication tools; ~~Password managers~~

3. Products with digital elements that support ~~with the function of~~ virtual private network (VPN) functions such as VPN server and clients;

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

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

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

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

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

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

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

6. ~~8.~~ Devices based on tamper-resistant integrated circuits, including embedded and integrated S~~s~~ecure E~~e~~lements;

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

8. ~~10.~~ Secure cryptoprocessors;

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

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

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

~~**Categories of products with digital elements which meet both the criteria referred to in Article 6(1 2), third subparagraph, points (b) and (c):**~~

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

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

~~10. Secure cryptoprocessors;~~

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

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

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

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

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

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

ANNEX [XX]

Simplified EU declaration of conformity

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

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

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

[…]

Italy

1. Scope

1.1 Exclusion clause

Concerning the exclusion clause (paragraph 5, article 2), our position is to rephrase the paragraph as in the box below.
Moreover, concerning the latest Presidency compromise proposal, our position is to reintroduce the previously added paragraphs 5b and 5c of article 2, while supporting the addition of paragraph 5 of article 4.
Finally, we support the introduction of an additional paragraph safeguarding domestic jurisdiction. A possible phrasing could be as follows "Member State may adopt or maintain provision with a view to achieving a higher level of cybersecurity of products with digital elements".
As per the "maintaining" of existing provisions, art. 114.4 and 114.6 of the TFEU might apply. The mentioned articles provide for a judicial basis to such a purpose, on grounds of major needs referred to in Article 36 (among them, national security is mentioned).

As per the "adoption" of (additional) provisions, a similar framework is provided for in directive 1535/2015.

Amendments 1: Article 2.

5. This Regulation does not apply to products with digital elements developed ~~exclusively for of national security, defence or military purposes or to products specifically designed to process classified information~~, **placed on the market, put into service, or used with or without modification for the purpose of:**

(a) activities which fall outside the scope of Union law;

(b) activities concerning military, defence or national security;

regardless of the type of entity carrying out those activities.
In addition, this Regulation does not apply to products specifically designed to process classified information.

5b. This Regulation is without prejudice to the Member States' responsibilities to safeguard national security or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

5c. The obligations laid down in this Regulation do not entail the supply of information the disclosure of which is contrary to the Member States' essential interests of

national security, public security or defence.

5d. Member States may adopt or maintain provision with a view to achieving a higher level of cybersecurity of products with digital elements.

1.2 Exclusion of non-connectable products with digital elements

As mentioned in our previous comments (WK 17303/2022), our position is to remove the scope limitation to only "connectable" products. That is, applying the Regulation to all products with digital elements independently from their capability to exchange data at the time of their placing on the market.
Therefore, paragraph 1 of article 2 would read as follows: "This regulation applies to product with digital elements". It greatly simplifies the text, making it future proof and less exposed to loopholes.

Amendments 2: Article 2, paragraph 1.

Article 2

Scope

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

This would also entail the deletion of the now unnecessary definitions of "logical connection", "physical connection" and "indirect connection" (paragraphs 11, 12 and 13 of article 3).
Mind that, taking into consideration the principles of proportionality, this slight increase in the scope is counterbalanced by the simplification in the conformity assessment procedures, reduction of initial critical products and fine tuning of the essential requirements (see section 5).

1.3 Exclusion of services and software as a service

While a national position has not been finalized yet, we are sceptical on the exclusion of services from the scope of the Regulation (paragraph 1, article 3), with particular emphasis on Sofware-as-a-Service (recital 9).
In this regards, we do not see major differences in between the mentioned services and the "remote data processing" and have some concerns in the application of CRA on products that leverage SaaS services (who is responsible for what?).
The changes in the recital 9 in the latest Presidency compromise proposal are proceeding in the right direction but may not be sufficient.
Therefore, we would welcome additional explanations by the Commission as well as continuing the discussion on this topic in HWPCI and are inclined to support the position of those Member States asking for the full inclusion of services and SaaS in the scope of the Regulation.

1.4 Open source

Recital 10 clarifies that "only free and open-source software […] supplied in the course of a commercial activity and therefore placed on the market should be covered by this Regulation.". While we agree with the overarching principle, we have two concerns with this provision:

1. inability for non-commercial open-source software to achieve the CE marking;
2. impact on the commercial services offered by companies that do not control most of the code-base of the non-commercial open-source software.

Concerning the former, we propose to introduce the possibility for non-commercial open-source software to undergo the conformity assessment to achieve the CE marking on a voluntary basis. This would also benefit:

- consumers that may therefore differentiate between open-source projects that are willing to undergo some scrutiny with respect to those that won't;
- open-source itself as its otherwise inability to achieve the CE marking may hamper its usage by consumer that may understandably associate the lack of CE marking as an indicator of untrustworthiness.

Concerning the latter, the current formulation (in combination with article 10, paragraph 4) may prevent the usage of open-source software in commercial product, as the companies that use open-source libraries or embed third-party open-source product would then be responsible to perform due diligence and ensure that the security of their product is not compromised by pieces of software they do not control and that are not subject to CRA requirements , which may not be technically feasible. This may in turn be a blow to innovation or research limiting the industrial usage of open-source.
We would welcome a discussion to address this issue.
A preliminary proposal to amend Article 24 is as follows:

Amendments 3: Article 24

4a.	**On a voluntary basis, for the purposes of applying the CE marking pursuant to article 22, products with digital elements not covered by this Regulation may demonstrate conformity with the essential requirements set out in Annex I by using any of the procedures referred to in paragraph 1.**

2. Interplay with other EU regulation

2.1 Interplay with Maritime and other sectoral regulations.

We would like to point out possible issues in the application of CRA with respect to products covered by Directive 2014/90 on marine equipment. We would therefore request a joint analysis on this topic by DG Connect, DG Move and DG Mare.
Generally speaking, we would welcome a broader analysis from the Commission to assess the impact of CRA with respect to EU legislation that tackles the concepts of conformity assessment and certification.

3. Reporting obligation

3.1 Notification process

Concerning the reporting obligation of manufacturer framework outline in article 11, the latest Presidency proposal (WK 5175/2023) did improve on the previous phrasing. Indeed, our position is

that vulnerabilities and incident notification must be notified directly to the CSIRT or national cybersecurity authority of the relevant Member State(s). This would also allow to promptly activate the already existing structures for cross-border cooperation at technical level (CSIRT Network) and operational level (CyCLONe) without introducing any additional mechanism, while also providing the opportunity for synergies in the implementation of the CVD policy that must be developed at national level under NIS2.
This is without prejudice to a possible subsequent notification of vulnerabilities from the Member State to ENISA, as provided by NIS2 in the context of CVD.
Further, we propose to align the notification timelines of both, vulnerabilities and incidents, to the ones of the NIS 2 Directive, with an early warning within 24 hours and a notification within 72 hours [insertion of paragraphs 1a and 2aa].
Moreover, we propose the following additional amendments to Article 11:

- MS may derogate to ENISA the management of vulnerabilities [insertion of paragraph 1b];
- Article 11 should not apply to vulnerabilities under the process of the NIS2 CVD [insertion of paragraph 1c].

Finally, the last Presidency proposal (WK 5175/2023) provides that the CSIRT Network submit notifications to EU-CyCLONe (Article 11(3)), instead of ENISA as in the previous formulation. We think that this is not appropriate for two main reasons:

- the cooperation between the CSIRT Network and EU-CyCLONe is established on the basis of procedural arrangements agreed upon by the two parties as provided by NIS 2 Directive (Articles 15(6) and 16(6)) and, therefore, this Regulation should not impose an exchange of information between these parties;
- this might possibly introduce delays in information flow to CyCLONe. Indeed, while the current formulation already requires national CSIRTs to forward notification to ENISA without undue delay (which in turn, as per the previous formulation, would submit the notification to EU-CyCLONe), there is currently no requirement for national CSIRTs to *promptly* forward notifications to the CSIRT Network.

Moreover, as the developer and maintainer of the European vulnerability database (pursuant to Article 12(2) of NIS 2 Directive), it is more natural that ENISA should be in charge of submitting notifications to EU-CyCLONe.

For these reasons, we propose to revert paragraph 3 of Article 11 to the previous formulation with regard to who is in charge to submit notifications to EU-CyCLONe.

Amendments 4: Article 11

Article 11 *Reporting obligations of manufacturers* 1. The manufacturer shall, without undue delay ~~and in any event within 24 hours of~~

~~becoming aware of it~~, notify **to the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure** ~~**in accordance with**~~**pursuant to Article** ~~**[Article X]**~~ **12(1) of Directive** ~~**[Directive XXX/XXXX (NIS2)]**~~**(EU) 2022/2555 of Member States concerned [through a single reporting platform]** ~~**to ENISA**~~ any ~~actively exploited~~ vulnerability contained in the product with digital elements. ~~The notification shall include **technical** details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken.~~

~~**ENISA**~~ **The CSIRTs** shall, without undue delay, unless for ~~**justified**~~ cybersecurity risk-related grounds, forward the notification to **ENISA** ~~**the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt**~~ and inform the market surveillance authorities **of all the concerned Member States** about the notified vulnerability.

1a. For the purpose of notification under paragraph 1, the manufacturer shall submit to the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555 of Member States concerned:

a. without undue delay and in any event within 24 hours of becoming aware of the vulnerability, an early warning, which shall include technical details concerning that vulnerability;

b. without undue delay and in any event within 72 hours of becoming aware of the vulnerability, a vulnerability notification, which, where applicable, shall update the information referred to in point (a) and, where applicable, shall include any evidence that the vulnerability has been exploited and any corrective or mitigating measures taken;

1b. By way of derogation of the first paragraph, Member States may delegate to ENISA the management of notification under paragraph 1.

1c. If the manufacturer is already engaged in a coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555 of Member States concerned with respect to a vulnerability, this article does not apply to the concerned vulnerability.

2. The manufacturer shall, without undue delay ~~and in any event within 24 hours of becoming aware of it~~, notify ~~**to ENISA the single point of contact designated or established in**~~

~~accordance with pursuant to Article [Article X]8(3)~~ **notify to the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555 ~~[Directive XXX/XXXX (NIS2)]~~ of the Member States concerned [through a single reporting platform]** any incident having impact on the security of the product with digital elements. ~~**ENISA**~~ **The designated** ~~single point of contact~~ **CSIRT** shall, without undue delay, unless for ~~**justified**~~ cybersecurity risk-related grounds, forward the notifications to ~~**the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned**~~ **ENISA and the single point of contact designated or established pursuant to Article 8(3) of Directive (EU) 2022/2555. The signle point of contact shall, without undue delay,** ~~and~~ inform the market surveillance authorities **in all concerned Member States** about the notified incidents. ~~The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact~~.

2aa. For the purpose of notification under paragraph 2, the manufacturer shall submit to the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555 of Member States concerned:

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

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

~~**2a. For all products with digital elements, the manufacturer shall have the possibility for the voluntary reporting of vulnerabilities of which active exploitation have not yet been observed.**~~

2b. In the case that a third party other than manufacturer discloses an actively exploited

vulnerability or an incident of a product under the scope of this Regulation to the CSIRT, the CSIRT shall without undue delay inform the manufacturer.

3. ~~**The EU CSIRT Network**~~ **ENISA** shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established ~~**by**~~**under** Article ~~[Article X]~~**16** of Directive **(EU) 2022/2555** ~~[Directive XXX/XXXX (NIS2)]~~ information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

3.1 Notification scope

Concerning the events that should be notified, our position is that, in addition to exploited vulnerabilities and incidents, manufacturer should also notify discovered vulnerabilities (see previous box, paragraph 1, Article 11).

4. Essential Requirments

4.1 Vulnerabilities management timeframe

The "Non-paper on a support period covering the entire expected product lifetime in the Cyber Resilience Act" (WK 2942/2023) already provides our current position.
While the latest Presidency compromise proposal (WK 3408/2023) implemented the comments related to blocks 1-2 of the abovementioned non-paper, we support also the inclusion of the comments to the other blocks, notably the introduction of the following amendment to Article 41, providing for Market surveillance authorities to publish statistics on expected product lifetimes provided by manufacturers:

Amendments 5: Article 41

8a. Market surveillance authorities may publish statistics about the average expected product lifetime, as specified by the manufacturer pursuant to article 10 (10a), per category of products with digital elements..

4.2 Requirement on third-party code

We think that an essential requirement should be added on third-party code access to the key functionalities of the product with digital elements. In particular, we propose to add a new letter to point 3 of Annex I, stating:

include controls on how third-party code can access key functionalities of the product.

5. Product criticality hierarchy, conformity assessment procedures and list of critical products.

The current framework defines four levels of criticality of products mapped to five "procedures" to demonstrate their conformity to the essential requirements (module A, module B+C or module H, harmonized standards, CSA).
The highly critical products mechanism introduces an ex-ante last resort option to cover non-anticipated situations, without resorting to the ex-post powers in article 45. Therefore, while the implementation may be improved, we are not against the underlying principle within the Regulation.
On the other hand, it may be argued that the distinction between ordinary, class I and class II products could be simplified and that three different procedures of conformity assessment reduce the differentiation in between the three levels.
With regard to the last Presidency proposal (WK 5175/2023), we welcome the deletion of the criteria regarding the intended use for essential entities under NIS2 for digital products of class II. Indeed, in our understanding, ensuring high level of cybersecurity within critical infrastructure should be handled under CSA (with certification) and NIS2 (with security measures) as they consider the criticality of product based on their context of usage. On the other hand, CRA should be aimed at ensuring minimum cybersecurity considering the intrinsic criticality of a product from a horizontal standpoint. Therefore, we would argue that, while usage in critical infrastructure may be considered in the reasoning to identify critical products, it should not be the main factor. For the same reason, we would remove the same criteria for highly critical products (Article 6a, let. (a)).
Moreover, considering that the most impactful provision of the CRA is the ex-ante third-party conformity assessment rather than the requirements themselves and that the list of critical products may be updated in the future, it would be safer to limit the number of product categories listed in Annex III. In this regard, we think that the latest Presidency proposal goes in the right direction, while we think that the categories of products listed in Annex III should be further reduced.
Moreover, we propose to:

1. remove the class I and class II distinction;
2. require that manufacturers of products of categories not listed in Annex III demonstrate conformity to the essential requirements set out in Annex I with third parties assessments (Article 24, par. 3);
3. require that manufacturers of products of categories not listed in Annex III demonstrate conformity to the essential requirements set out in Annex I by applying harmonized standards, where they exists;
4. review the list of categories of products, from cumulatively 33 to roughly 10. Also, considering that the Regulation does not define the categories of products, which are, thus, sometimes subject to interpretation. Specifically, we believe the list could be limited to:
   - General purpose boot managers;
   - General purpose hypervisors;
   - General purpose operating systems;
   - General purpose microprocessors;
   - Firewalls, intrusion detection systems and intrusion prevention systems;
   - Antimalware/Antivirus;
   - VPN servers and clients.

This approach would simplify the regulation, reducing the number of procedures and categories to be fine-tuned, while also avoid overloading the industry, the national authorities, and the notified bodies in the initial application of the CRA.

6. Delegated Powers

The latest Presidency compromise proposal (WK 5175/2023) extend to an indeterminate period of time the power to adopt delegated acts conferred to the Commission (Article 50, par. 2). While the 2 years limit as for the previous formulation does not appear coherent with the timeline for the entry into force and application of the Regulation, we think that the power to adopt delegated acts should be conferred to the Commission for a determined period of time, sufficiently larger than the entry into force and application of the Regulation, while limited, appropriately, by the expected period for the review of the Regulation.

Hungary

Recital (11a)

In Recital (11a) we propose to change the wording „distribution" to „download", since certain software vendors use a mesh network between endusers to distribute software updates, and therefore endusers also have to provide upload bandwidth in order to participate in the distribution network. Security updates should be made available to users also in a download only manner, without taking part in a two-way distribution network. We also propose to introduce the opt-out possibility for the downloads of software updates, not just the installation.

„(11a) 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 create processes to ensure that internet-connected products with digital elements include functions that enable the notification, distribution**, download** and installation of security updates automatically. They should also provide the possibility to approve the **download and** installation of the security updates as a final step, as well as clear instructions on how users can opt out of automatic updates. The requirements relating to automatic updates laid down in Annex I of this Regulation are not applicable to products primarily intended to be integrated as components into other products. They also do not apply to products for which users would not reasonably expect automatic updates, including in critical environments where an automatic update could cause interference with operations, such as in industrial environments."

Recital (19a)

When drafting the text of Recital (19a), we propose to take into account the possible conflict between compliance and security requirements, with special regards to the case of emergency security updates of vulnerabilities being actively exploited, even if it temporarily breaches compliance with security standards (e.g. OpenSSL and RSA BSAFE vulnerabilities being actively exploited, while security patch is technically available, but not yet certified for FIPS 140-2).

Netherlands

Recitals

Recital 9: Scope and SaaS

We still believe that more clarity on the scope regarding Software-as-a-Service (SaaS) in this recital would be desirable. An alternative could be to discuss various examples in Commission communication, for example in guidelines provided to economic operators on the scope and how to apply the CRA.

No additional comments regarding the recent amendments.

New recital corresponding to art 4 para 1

We support the added explanation given in this recital. The CRA only regulates the requirements that have to be met in order to make products with digital elements available on the market, and does not hamper Member States in applying additional requirements for the use of certain products with digital elements in certain situations or in case of public procurement regarding products with digital elements. We also agree that non-technical factors relating to (manufacturers of) products with digital elements are not covered by the CRA, allowing Member States to lay down national measures regarding non-technical factors that for example can include restrictions on the use of products from high risk vendors in certain situations. An example would be products used in specific parts of private mobile networks that could pose national security threats if supplied by high risk vendors.

New recital corresponding to art 4 para 5

We support the idea that Member States should be able to subject products with digital elements that will be used for military, defence or national security purposes, to additional measures, and can support the proposed recital.

Recital 9a: remote data processing solutions

We support the proposed recital 9a, but it should directly follow recital 9 which also describes remote data processing solutions.

Recital 10: commercial activity / open source

As mentioned before we welcome the compromise text for recital 10.

However, we still would like to propose alternative wording for the last 2 sentences of this recital because we think they can be confusing. The phrase starting with "taking into account of" seems to imply that the CRA only applies to Open Source that matches the definition *and* is offered on a commercial basis. Which is not the case, because the CRA also applies to all other commercial software. Something similar is the problem with the phrase that starts with "For the same considerations". No activity that charges a fee solely for the recovery of actual costs is considered a commercial activity. This is not limited to public administration activities.

We therefore suggest to amend the text as follows:

> (10) This Regulation applies only 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. The supply in the course of a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise, by providing a software platform through which the manufacturer monetises other services, or 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. The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity. **Open-source software is understood as free software that is openly shared and freely accessible, usable, modifiable and redistributable, and which includes its source code and modified versions.** Taking account of the above-mentioned elements determining the commercial nature of an activity~~, only free and open-source software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable, supplied in the course of a commercial activity and therefore placed on the market should be covered by this Regulation.~~ **this Regulation should only apply to open-source software that is supplied in the course of a commercial activity.** ~~For the same considerations, p~~**P**roducts provided ~~by public administration entities~~ as part of the delivery of a ~~public~~ service for which a fee is charged solely to recover the actual costs directly related to the operation of that service**, as is often the case with products provided by public administration entities,** should not be considered on those grounds alone a commercial activity for the purposes of this Regulation.

Another suggestion that was made by stakeholders we spoke to, is to clarify, in a recital, the role of platforms and under what circumstances a platform should be considered to be a 'distributor' in the CRA. These platforms are used by developers to offer or supply their software to the public, from which other developers, commercial manufacturers or end users can download this software. As long as the platform does not charge a price or in other ways applies commercial conditions for the downloading and use of the software from its platform (which *would* be the case with app stores), this does not constitute the 'making available' of products with digital products, and the platform should not be considered a distributor under the CRA. We propose to add the following wording to recital 10 or make this a new recital 10a:

> (10a) Free and open-source software is developed, maintained, and distributed via online platforms. A package manager, code host or collaboration platform that facilitates the development and supply of software is only considered to be a distributor if he makes this software available on the market, hence supplies the software for distribution or use on the Union market in the course of a commercial activity.

Recital 11a

We very much welcome the recital on automatic updates. In our view, the requirement to provide products with automatic updates as the default setting however shouldn't apply to *all* products with digital elements as setting it as a default would cause problems in professional settings.

So slight amendment to get this straight.

The chance of disruptions to the continuity of organisations is high if an update is initiated outside the control of network administrators. This is not only true for critical or industrial environments, but also applies to other professional ICT-networks. We therefore propose to amend the last sentence in recital 11a as follows:

> They also do not apply to products for which users would not reasonably expect automatic updates, including **in professional ICT-networks, and especially in** critical **and industrial** environments**,** where an automatic update could cause interference with operations.

Recital 18a: due diligence

We welcome a recital on the due diligence obligation in article 10 para 4, and we support the risk based approach to this due diligence. In the case of a manufacturer integrating a component that is itself regulated under the CRA, it makes sense to suffice with the obligation to check if the component manufacturer is in conformity with the CRA, for example by checking the CE label. However, if the component to be integrated is not regulated, because it is not supplied in the course of a commercial activity (non-commercial open source for example), we want the recital give some more guidance on *how to determine the level of effort required* from integrators of non-commercially supplied components. When are efforts sufficient to fulfil the due diligence obligation? We understand that the ways to do this should be left open, but we should give more guidance on the level of effort required.

A second suggestion for this recital is to mention the fact that the responsibility of the manufacturer integrating a component sourced from a third party does not stop after the due diligence during the integration, which typically would occur at the moment of placing on the market. He will also continue to be responsible for the effective vulnerability handling during the expected product lifetime.

We propose to add the following wording regarding the responsibility for vulnerability handling to recital 18a:

> The responsibility of the manufacturer integrating a component sourced from a third party does not stop after the due diligence during the integration, which typically would occur at the moment of placing on the market. He will also continue to be responsible for the effective vulnerability handling during the expected product lifetime.

New recital 19a: actively exploited vulnerabilities

We welcome a recital on actively exploited vulnerabilities. Following last week's workshop on reporting obligations and the benefits and risks that were presented by the Dutch NCSC, we think this recital should include the following:

- A further explanation of what is meant by actively exploited vulnerabilities complementary to the definition given in article 3 (39). For example, this definition should not be contrary to (multiparty) CVD-policy since in the current definition of article 3(39), an ethical hacker or researcher may potentially fall under the current definition. We should make sure that this will not be the case and will refer to this in our written comments.
- Even more, this recital should state that the risks of reporting unpatched vulnerabilities should be minimized by technical measures and procedural agreements. An example of a technical measure is the security of the reporting platform. Examples of procedural agreements can be setting up rules and procedures on what information regarding a vulnerability is shared and under which classification (screening of staff/ EU-secret level). Also clearly defined cyber security risk related grounds can help minimize those risks.

Recital 22 and 22a: substantial modification and security updates

We welcome the clarifications in order to take away the misconception that every minor update would cause the need to undergo a new assessment. However the last sentence could also be read too absolute: not every combination of a security and feature update will be a 'substantial' modification. Also, the word *significant* should be *substantial* as that is the term used in article 16.

> In assessing whether an update is considered a substantial modification it is not relevant whether the feature update is provided in a separate software update or combined with a security update.

Recitals 25, 26, 27

See comments regarding article 6, no specific comments regarding the recitals.

New recital 32a

We welcome recital 32a that discusses how to apply the essential requirements in Annex I. We would however prefer to add the explanation given by the Commission during the HWPCI meeting on 15 March: a product that would not be able to comply with a specific essential requirement without having to add a functionality to it, is in that case not required to add that functionality. This discussion has taken place in the course of the drafting of the standards under the RED Delegated Act, so it would be helpful to clarify this here beforehand.

We would also again like to suggest mentioning in this recital that the requirements will need to be worked out in harmonised standards in which *state-of-the-art* technical measures to meet these requirements will be prescribed.

Recitals 34 and 35: reporting obligations

These recitals will need to be amended based on changes for article 11 on reporting obligations. We provide suggestions for amended corresponding recitals under article 11.

Recital 41, 41a / article 18

We welcome the additions to this recital, clarifying that common specifications should only be adopted if serious attempts to let the market draft harmonised standards fail. Also we welcome mentioning the involvement of relevant stakeholders once common specifications are to be established.

Recital 41b / article 18

The explanation that the reasonable period in the proposed text for article 18 para 3 sub b is a period of 1 year max could be inserted in the para itself, which would be much clearer than this recital. If a recital is deemed necessary, some introduction to the term 'reasonable period' is necessary, and it would be better to cut this paragraph into more than one sentence to improve readability.

New recital 67a

We support this recital and the corresponding article.

Articles

Article 2 and 4 regarding national measures versus maximum harmonisation

As was discussed during last meeting of the HWPCI, an important principle to be held in mind is that the CRA only regulates *the making available of* products and does not regulate the *use* of products. As long as a national measure does not limit the free movement of products that comply with the CRA on the internal market the national measure would not conflict with the maximum harmonisation of the CRA. MS should therefore be allowed to require higher CS requirements for products to be used in certain situations, for example in national regulation aimed at the security of mobile networks or other NIS entities, or in public procurement procedures. Another national measure that should not conflict with the maximum harmonisation in the CRA would be to ban specific products based on non-technical reasons, not only because national security is a MS prerogative, but also because this is not covered by the CRA and therefore no maximum harmonisation regarding non-technical measures exists. This seems to be correctly addressed in the current wording of the recitals corresponding to articles 2 and 4.

Article 3

We would like to further clarify the definition under (2):

> 'remote data processing' means any data processing at a distance for which the software or hardware **of the product with digital elements including its remote dataprocessing part** 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;

Under (7): "capable of processing …digital data" can be removed, since it was already included under 'electronic information system'.

> 'hardware' means a physical electronic information system, or parts thereof ~~capable of processing, storing or transmitting digital data~~;

Article 6 and 6a

The exact relationship between the category of highly critical products and Annex III is not clear to us. Can products that fall under Annex III – which includes the most fundamental digital products – also fall under highly critical? What does that mean for the conformity procedures? Do manufacturers have to satisfy both those of Annex III and obtain a CSA certificate?

The difficulty is that we do not know what products will fall under highly critical. The bar far achieving conformity in this category is high: CSA certification schemes are hard to obtain for smaller companies. Therefore it is necessary to have more clarity on what products will be included. And when will these schemes be available? Based on what we have seen with the CSA this may take many years. What will we do in between? This is a part of the text which still raises many questions, also for private parties.

We do see merit in trying to make the CRA and CSA work well together. But the current text needs further clarification on the relation between Annex III and the highly critical category, and also on what products Commission would be putting in this highly critical category.

Article 10 – Obligations of manufacturers

In the meeting of the HWPCI on 15 March it was clarified by the Commission that the manufacturer is in fact intended to be responsible for the vulnerability handling in case a vulnerability is identified in an integrated component sourced from a third party. We think this is not yet clear in the proposal, as we understood that the CRA only addresses the responsibility of the integrator in 2 instances:

- article 10 (4) prescribes exercising due diligence when integrating of components in order to comply with the prescription in article 10 (1) to ensure that the product with digital elements has been designed, developed and produced in accordance with the essential requirements,
- and article 11 (7) prescribes the reporting of an identified vulnerability in a component to the person or entity maintaining the component.

As suggested before, we would like to clarify that the manufacturer is imposed with more responsibilities regarding the component he chooses to integrate in his product. If a full responsibility to ensure that the product including all of its components (also the ones sourced from third parties) has been designed, developed and produced in accordance with the essential requirements (article 10 para 1) would not be proportionate, the manufacturer should at least be responsible for the effective vulnerability handling in article 10 para 6. This means that a manufacturer cannot suffice with the reporting of an identified component to the person or entity maintaining a not-regulated component: he should also make sure the vulnerability is handled effectively (either by himself or the person or entity maintaining the component).

Our previous text proposal to add this notion in article 10, para 6, was unintentionally limited to not-regulated components. We would therefore like to correct our previous text proposal:

> 6. Manufacturers shall ensure, when placing a product with digital elements on the market and for the expected product lifetime, that vulnerabilities of that product ***including all of its components,*** are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

In response to the issue raised by the Commission in the last HWPCI we are currently reflecting on a solution for specific situations in which the requirement to handle vulnerabilities for the duration of the entire expected product lifetime becomes disproportionate, for example when the product would in theory have an indefinite product lifetime, or when the product is used by a very small number of users which would make vulnerability handling unrealistically burdensome. This could be described in the corresponding recital, for which we will provide a text proposal at a later stage.

Also, we would like to add some more nuance to para 13:

> They shall cooperate with that authority, at its request, on any measures taken to ~~eliminate~~ **adequately reduce** the cybersecurity risks posed by the product with digital elements, which they have placed on the market.

Article 11 – reporting obligations of manufacturers

The current compromise text remains unclear and leaves too much room for interpretation regarding the structure of reporting. With the negotiations proceeding, we would like to stress the urgency and importance towards other Member States to further discuss this complex issue and together find a workable formulation of article 11. We would like to refer to a separate options paper on reporting obligations that we have shared with the Presidency.

Articles 18 and 19

We welcome the proposed amendments to articles 18 and 19. It should be made clear that harmonised standards are by far the preferred procedure, and that common specifications should only be adopted if serious attempts to let the market draft harmonised standards fail.

Art 18 para 3: The explanation in recital 41b, that the reasonable period in the proposed text for article 18 para 3 sub b is a period of 1 year at a maximum, could be inserted in the para itself. This would be much clearer than the recital. Proposal:

> (b) no reference to harmonised standards covering the relevant essential 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 **year** ~~reasonable period~~.

[However, the procedure described here (to our understanding) would not fit in the implementation period of 24 months, unless it would be clear after one year already that a harmonised standard will not be accomplished within the next year.]

Art 18 para 9: for products not listed in Annex III a CSA certificate at a lower assurance level could suffice. Therefore we don't support the addition of the words *at assurance level "substantial" or "high"* here.

Article 38 – Information obligation on notified bodies

Article 38 prescribes notified bodies to inform the notifying authority of (among other things) any suspension or withdrawal of a certificate. We think this information would be especially relevant for market surveillance authorities.

We propose to include an information obligation to also inform *market surveillance authorities* by adding a paragraph 3 to article 38:

> **3. Notified bodies shall inform the market surveillance authorities of any refusal, restriction, suspension or withdrawal of a certificate.**

Article 45 – Procedure at EU level regarding products presenting significant CS risk

We maintain a scrutiny reservation on the proposed competence for the Commission. It is important that the Member State maintains its responsibility for its market surveillance, whilst keeping in mind the importance of cooperation between Member States. We want to stress the importance of the independent role of market surveillance authorities.

We therefore propose to at least add more safeguards to better reflect that this would be a 'last resort' measure. Examples could be to prescribe in para 2 that the Commission procedure should start with a consultation of the national market authorities asking them for their reasons not to take measures and allowing national market authorities to act themselves within a specific timeframe. Another example of additional safeguards could be to introduce an objection procedure similar to the objection procedure for national market surveillance authorities in Article 44.

Article 57 – Entry into force and application

Without a suitable standard for its product with digital elements, it will be practically impossible for a manufacturer to use self-assessment. Conformity assessment bodies would be inundated with assessment requests, not only for critical products but also for all products with digital elements for which there is no suitable standard available yet.

Considering the wide variety of products with digital elements that will be in scope of the CRA it will not be possible to draft one standard that would fit all of them, so we will need to finish various standardisation procedures before the date of application**.** We should consider that the group of experts working on the drafting of one standard will largely overlap with the group of experts needed to draft the other standards under the CRA, so it is difficult to simultaneously work on different standards. Moreover, as we understand, there are no standards for cybersecurity of software yet and this novelty could proof to be particularly challenging.

For the CRA to become a success it is crucial that a realistic timeframe is provided, taking into account not only the drafting time but also the procedure of Commission approval and the implementation by manufacturers of harmonized standards once they are available.

Looking at the current experiences in the standardisation process for the Radio Equipment Directive (RED), we have doubts whether 24 months for the CRA is a realistic timeframe. The implementation period for the RED was 30 months, and a delay of 12 months is requested. As the RED requirements are laid down in a delegated act, such delay could be granted. As the application date of the CRA could only be altered by an amendment of the legislation, it should be carefully chosen in advance, with the risk of delayed standardisation processes in mind.

Without taking a formal position on this issue yet, we suggest an implementation period of 36 months for the CRA. Furthermore, considering the specific challenges expected during the standardisation process for software, we suggest an implementation period of 48 months for software products.

Annexes

Annex I – Essential cybersecurity requirements

Regarding part 1 sub 3 a: We support adding the text regarding automatic updates by default, however it is necessary to limit this requirement to consumer products. For non-consumer products, a voluntary opt-in for automatic updates could be an alternative to an opt-out of automatic updates. If this is not carved out in the essential requirement itself, it would be necessary to explain this in the corresponding recital 11a. We refer to our comments regarding recital 11a.

A smaller issue: the referral to Annex II 8a seems incorrect, and we don't understand "according to requirement in Annex II 8a", because this does not seem related to the type of technical security support offered by the manufacturer.

Annex II – Information and instructions to the user

Regarding sub 9a: We should not include 'expected' here. This refers to the secure use of a product, so these instructions should not be limited to the support period in article 10 para 6, which uses the term 'expected' product lifetime.

Regarding sub 9e: We would like to insert 'where applicable'.

Regarding sub xx: we do not see sufficient reason to prescribe the way in which the SBOM should be provided to users, considering that the inclusion of an SBOM is a voluntary decision of the manufacturer.

Annexes I and II

A general remark regarding the Annexes: it would be good to check on consistency of the wording of (for example) information obligations that are described in both an article and in the Annexes.

Annex III – list of critical and highly critical products

The proposed rearrangement of the list in Annex III is an improvement to clarify what criteria were considered in the decision to place a certain product in Annex III as either critical or highly critical.

We maintain a scrutiny reservation regarding the contents of the list.

Finland

Finland would like to thank the precidency for the new compromise text and the good work done so far. We have the following comments to the text. Our edits to the text are marked in red to make it easier to follow the changes.

Articles

Article 3

In many discussion during negotiations there has been a request to specify the relationship of products and services. We would like to propose a slight specification to definition of product with digital element as follows:

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

Adding a word "copy" relating to a software would separate it from a service that also by definiton can be "an electronic information system that consist of computer code". The difference between a product and a service is that software products are copies of that code and services grant access to the service and does not share a copy of a code. The problem using only wording "software product" is that it can also be understood as SaaS. Therefore we would like to add the word copy just to clarify this issue.

The justification to change "and" to "including" is to make clear that remote data processing solutions always need to be connected to the product. Now the wording is slightly unclear and we feel that this would clarify the text as we see that it ment to be understood.

Also we would like to suggest change to the definition of actively exploited vulnerability to clarify more what is meant by it.

(39) 'actively exploited vulnerability' means a vulnerability under active exploitation for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner that can be attempted or successful.

Additionally the definition of attempt or successful exploitation could include the following criteria that could be reflected in the recital or elsewhere.

1) In attempted exploitation the attacker executes malicious code but the code doesn't execute or obtain target information

2) Successful exploitation by vulnerable code allows the attacker to perform additional, unauthorized actions to the system or network

Article 6

We can support the new approach in article 6 and we think that it now focuses more to the point of the article. We have some minor suggestions for paras 1 and 2 to make it easier to read:

(1) ~~**Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements.**~~ Products ~~which have the core functionality of a~~

~~category~~ that ~~is~~ are listed in Annex III to this Regulation shall be subject to the conformity assessment procedures referred to in Article 24 (2) and (3). ~~**be considered as falling in belonging to that category.**~~

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

FI cannot support the changes made in paragraph 3 on delegated power. The paraghraph is now very open on the mandate. We think the paraghaph needs to be much more specific. Our general concern on this delegated power has been the legal certainty of it and wheter this is possible to establish via delegated act. Delegated acts can only add or delete non essential elements of the legislative act and from our point of view this delegated power that creates obligations from self assessment to third party assessment could potentially have impact on the key elements of the proposal. Amending list in Annex III would have major impact on manufacturers' costs of compliance with the proposal.

We would like to propose the following changes:

[The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including a new product with digital element in class I or class II, changing products with digital element from one class to another or remowing products from Annex III. When assessing the need to amend the list in Annex III, the Commission shall found/establish the amendment on the criteria referred to in paragraph 2 of this Article and assess the cybersecurity risks of the products. Prior to adopting the delegated acts the Commission shall consult the Member States and relevant stakeholders of the scope and content of the amendment and takes the results of the consultation into account when adopting a new delegated act.

We would also like to have an opinion of Council Legal Service whether or not this kind of delegated power would affect to essential parts of the regulation. This would also apply to the delegated power related to Annex I and Article 6 a.

Article 6 a

We thin the delegated power of Art. 6 a needs further specification since "take into accout" it too ambiguos with its interpretation. Also the paragraph refers to "categories of highly critical products" our understanding is that there are no different categories – just products. Therefore we would like to propose following changes:

The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying ~~categories of~~ highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate **at assurance level 'substantial' or 'high'** under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such ~~categories of~~ highly critical products with digital elements, the Commission shall ~~take into account~~ found/establish the delegated act on criteria referred to in paragraph ~~**1**~~2 of ~~**this**~~ Article 6 ~~**the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2,**~~ as well as ~~**in view of the assessment of whether that category of products is**~~ **any of the following criteria**: - -

We also think critical supply chain need further defining in subparagraph (b). What would constitute critical, to whose critical supply chain would need to be affected and what would serious disruption mean? Would these also be related to NIS2 essential entities or other sectors too?

Article 10

Given that the product lifetime has been changed from maximum of five year to the whole lifecycle some adjustments need to be made through out the Regulation. There are several references to 10 year limit of keeping the documentation available after the product has been made available on the market. These paragraphs are the following:

Art. 10 (6) – this is not about the documentation but might need adjusting anyway
Art. 10(8)
Art. 13(7)
Art. 17(2)
In Annex VI
Module A para 4.2
Module B para 9
Module C para 3.2
Module H para 5.2

The following phrase should be added to all of these: *or for the expected product lifetime, whichever is longer.*

Also, in paragraph 11 there is a requirement concerning the simplified EU declaration of conformity. It now states that it needs to be included in the instructions. Compaired to the RED DA this requirement is "Manufacturers shall ensure that each item of radio equipment *is accompanied by* a copy of the EU declaration of conformity or by a simplified EU declaration of conformity." We propose changing the wording of the text according to the RED DA since in some cases it might give more flexibility to the manufacturer but would still provide the user the same amount of information as the current formulation of the text.

Article 11

Since the precidency has a separate meeting on the topic of art. 11 we would like to take a little more time to assess the questions sent to the working party and provide answers to those questions in writing after the meeting.

However, we can already provide some general points that reflect some of our views to the topic. For one, we think that the 24 hour timeframe in the article is too short from practical point of view. Also, it might be less burdening if the reporting would focus on confirmed vulnerabilities and incidents since there is a chance of false positives and it might be good to give the manufacturer some time to assess the situation and confirm that there is indeed an actively exploited vulnerability or an incident. This would most likely save resources from all parties involved.

We also think actively exploited vulnerability might need further assessing as a term and we have suggester under art. 3 a new, slightly different definition.

Article 16

We would like to make sure that the wording "for the purposes of this Regulation" does not cover modifications done for private purposes or research and development purposes i.e. it means that after modification there still needs to be "placing on the market" in order to the obligations to apply according to art. 16?

Article 24

We think that taking account the SMEs when putting the regulation into force is important. However, we think that para 5 is problematic in terms of equal treatment and "taking into account" is vague with interpretation. This might also quite easily lead incoherent pricing through the EU. Therefore we cannot support this paragraph without hesitation and other support mechanisms should be evaluaded aswell.

Article 53

We would support assessing this article in the light of what was proposed by Estonia on the sanctioning when there is a third party assessment done and the penalty is based on non-compliance of requirements laid down in Annex I.

Article 57

We have a cautious approach to the time of starting the application of the Regulation. The time for starndardisation and certification schemes has proven to be difficult and the planned schedule is ambitious to begin with.

Recitals

Recital 9

We would like to suggest some clarifying suggestions to recital 9 following our proposal on Art. 3 on definitions. Our aim with these suggestions is to clarify the scope of the remote data processing.

(9) This Regulation ~~**ensures a high level of cybersecurity of products with digital elements. It does not regulate services, such as Software-as-a-Service (SaaS), except for**~~ applies to remote data processing solutions ~~relating to~~ included in a product with digital elements, ~~**understood**~~ defined as any data processing at a distance for which the software **or hardware** is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions. - - -

New recital corresponding to Art.4, para 1

We can support the new text on the recital. We think, in terms of accurancy it could be good to clarify that the further *cybersecurity* requirements cannot be imposed by the Member States.

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 further cybersecurity requirements for the making available on the market of products with digital elements. Entities can however establish additional requirements to those laid down by this Regulation for the procurement or use of those products for their 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. - -

Recital 9 a

We think that recital 9 a would be more logically placed directly after recital 9 and before new recitals that are currently without a number in the text.

Recital 11 a

We think tha term *internet-connected product* creates a new cathegory of products and we think this is not necessary. The words “internet-connected” could be deleted since it is clear that automatic updats cannot be done without access to the internet anyway.

Recital 15

Based on our analysis there is a difference of exclusion clauses in RED Delegated Act and the CRA Art. 2. RED art. 3 sets essential requirement for Radio equpment and according to RED Delegated Act regarding these essential requirements contains some exclusion clauses than CRA – Regulations (EU) 2017/745 and (EU) 2017/746 **but not** (EU) 2019/2144. We were not able to analyze further this issue before the deadline but we’ll come back to this later on if something comes up. This might be relevant especially when it comes to conformity assessment requirements if RED DA would be repealed.

New recital after Recital 17 on Data Act

Since data is acting an important part of what is protected with cyber security requirements a note should be made on the relationship of this regulation to Data Act and also to NIS2 directive. The Data Act (in its current form) regulates for example data processing services that may be overlapping with remote data processing solutions of CRA. Since the Data Act also has requirements concerning security, this is something that needs to be addressed in the CRA. Also these service providers in many cases fall under NIS2 scope.

Our understanding is that NIS2 covers most of the cloud service providers, their risk management and security measures related to that, CRA covers products that may use cloud services as part of their functionality (remote data processing) and therefore some parts of the security requirements may arise from CRA. Then Data Act covers security measures of generated data for example by IoT devices and cloud service providers. We think that it is important to clarify the relationship of the three regulations in a way that it is clear what is applied and to what extent. At this point it is not quite clear if the requirements are overlapping or not and this is something that needs attention in the further work. We also keep doing further analysis on this but at this point we would like to point this out as and issue that needs to be clarified hopefully in the end in a form of a recital. Unfortunatelly we did not have the chance to formulate it to this round of comments.

Recital 22 a

We think it would be useful to add some text on regular maintenance updates that would not be a feature update but are not necessarily safety updates either and would not constitute a substantial change.

Also it might be worth thinking a situation where a security update (perhaps featured by a feature update) would constitute a substantial change and this change would require a third party assessment. This might however be a hypothetical situtation. Should the urgency of the security update be prioritized to third party conformity assessment procedure? In that case if something would come up in the conformity assessment that would be fixed later on.

Recital 27 a

See our comment on critical supply chain under Art. 6 a.

Recital 41 b

It remains unclear to what does the “reasonable period” refer to?

New recital on online market places

It might be good to have a expanatory recital on the online marketplaces as discussed in the previous meetings. Our understanding was that the regulatory frame would come from the General Product Safety Regulation and the Blue Guide but this would be informative to write to the text since it is quite relevant in the context of digital products such as softwares.

Annexes

Annex III

We would like to return products used in OT-environments returned to Annex III. These would be

Class I

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

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

Class II

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

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

14. Robot sensing and actuator components and robot controllers;

Some additional comments:

We got a question concerning whether or not electronic communications networks would constitute as a product falling under the scope of the CRA and would the providers of networks constitute manufacturers in that case. The answer to this question remained unclear to us and we would like to ask whether this is something that has been thought during the drafting process.

The providers of electronic communications networks would fall under the scope of NIS2 and our initial thought is that they would not be considered manufactures in the context of the CRA but we would like to get a confirmation to this question.

Another note concerns standards. Article 18 now only takes a position on European standards but our view is that the market would benefit more widely on the application of international standards. We understand that international standards can be adopted as European standards that are published in the official journal an sthe other way around but our question is that does the current formulation of the proposal limit too much of the use of international standards? Or is the intended methology of using international standars to adopt them into European standards where approppriate?

On a final note, we are doing some assessment on the proposal in relation to the nuclear sector regulated under the Euratom-treaty since some sectoral specifities may be possible given the different treaty. Unfortunately we were not able to come up with any conclusions whether or not this - in our opinion - would need any further attention.