European Parliament
2019-2024

Committee on the Internal Market and Consumer Protection

2022/0272(COD)

30.6.2023

OPINION

of the Committee on the Internal Market and Consumer Protection

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council on Horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Rapporteur for opinion (*): Morten Løkkegaard

(*) Associated committee – Rule 57 of the Rules of Procedure

PA_Legam

SHORT JUSTIFICATION

As the former Rapporteur for opinion in the IMCO Committee on the NIS2 Directive, the Rapporteur sees the Cyber Resilience Act as a crucial and natural next step to improve the cybersecurity of the European Union. Being mindful that by definition cyber security will never be 100 per cent complete, the Rapporteur is of the opinion that it is important that everything within our power is done to decrease the number of weak links in our Union, and for this the Cyber Resilience Act is a welcomed next step. We need to increase the cybersecurity of the products with digital elements and other new products such as IoT devices that have become natural parts of the everyday lives of European consumers and businesses.

As the IMCO Committee is responsible for the functioning and implementation of the Single Market, including the Digital Single Market, and rules on consumer protection, the Rapporteur sought to introduce amendments that aim to improve the functioning of the internal market, while providing for a high level of consumer protection within the scope of the proposal, specifically with regard to cybersecurity requirements for products with digital elements.

Furthermore, the Rapporteur believes that some aspects of the proposed Regulation require improvement to ensure legal clarity and coherence between the relevant provisions of the proposed Regulation and other pieces of legislation. This relates in particular to the NIS2 Directive, the recently adopted General Product Safety Regulation, the Artificial Intelligence Regulation, and the Machinery Regulation, as well as a number of relevant delegated and implementing acts. Therefore, the Rapporteur proposed amendments that aim to improve legal clarity and help to ensure coherent, effective and consistent interpretation and application of the mentioned legislations.

Moreover, as micro, small and medium sized enterprises are crucial economic players in the digital market, the Rapporteur introduced a number of amendments to simplify administrative procedures and limit the administrative burden on small businesses, without lowering the level of safety. Furthermore, the Rapporteur introduced amendments that ensure that micro-enterprises and SMEs, will be provided with specific guidance and advice in complying with the requirements in the Cyber Resilience Act.

Finally, the Rapporteur has introduced amendments with the aim of ensuring more efficient communication with competent authorities (national market surveillance authorities, ENISA), as well as strengthening the provisions for the obligations and competences of relevant authorities with regards to complaints, inspections and joint activities. Further to this the some amendments by the Rapporteur focus on improving the cybersecurity requirements for components integrated into final products with digital elements, specifying the obligations of economic operators, such as manufacturers and authorised representatives.

The Rapporteur reiterates the position that the introduction of the Cyber Resilience Act is a timely and natural next step to tighten the net around cybersecurity threats in our Union. With the suggested amendments, the Rapporteur has sought to find the right balance between ensuring an increased level of cybersecurity to the benefit of European consumers with a proportionate burden on the business community. It is the ambition of the Rapporteur that cybersecurity will become a natural parameter of competition in the internal market. It is with this in mind, that the Rapporteur has sought to adjust the proposal.

AMENDMENTS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a regulation
Recital 1

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

Amendment 2

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered as	(7) Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered as

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

Amendment 3

Proposal for a regulation
Recital 7 a (new)

Text proposed by the Commission	*Amendment*
	(7 a) This Regulation should not apply to the internal networks of a product with digital elements if these networks have dedicated endpoints and are completely isolated and secured from external data connection.

Amendment 4

Proposal for a regulation
Recital 7 b (new)

Text proposed by the Commission	*Amendment*
	(7 b) This Regulation should not apply to spare parts intended solely to replace defective parts of products with digital elements, in order to restore their functionality.

Amendment 5

Proposal for a regulation
Recital 9

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

Amendment 6

Proposal for a regulation
Recital 10

Text proposed by the Commission	*Amendment*
(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.	(10) ***Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. Research by the Commission also shows that free and open-source software can contribute between €65 billion to €95 billion to the Union's GDP and that it can provide significant growth opportunities for the European economy.*** 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. A commercial activity***, within the understanding of making available on the market,*** might ***however be characterised*** by charging a price for a ***free and open-source software component***, but also by ***monetisation like*** charging a price for technical support services***, or paid software updates, unless this serves only the recuperation of actual costs***, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. ***Neither the collaborative development of free and open-source software components nor making them available on open repositories should constitute a placing on the market or putting into service. 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. When open-source software is integrated into a final product with digital elements that is placed on the market, the economic operator that has placed the final product with digital elements on the market should be responsible for the compliance of the product including of the free and open-source components.

Amendment 7

Proposal for a regulation
Recital 11

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

Amendment 8

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(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.	(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, ***when*** the Commission repeals ***the*** 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.

Amendment 9

Proposal for a regulation
Recital 18 a (new)

Text proposed by the Commission	*Amendment*
	(18 a) In order to ensure that individual or micro developers of software as defined in Commission Recommendation 2003/361/EC do not face major financial obstacles and are not discouraged from testing the proof of concept as well as the business case on the market, these entities should be required to make best efforts in order to comply with the requirements in this proposal during the 6 months from placing a software on the market. This special regime should prevent the chilling effect of high compliance and entry costs could have on entrepreneurs or skilled individuals who consider developing software in the Union. However, this special regime should not apply to highly critical products with digital elements.

Amendment 10

Proposal for a regulation
Recital 19

Text proposed by the Commission	*Amendment*
(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	(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 ***by means of an early warning,*** of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having ***a significant*** 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

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

with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and ***immediately*** inform the relevant market surveillance authorities about the ***existence of a vulnerability and where applicable, the potential risk mitigation measures. Where a*** notified vulnerability ***has no corrective or mitigating measures available, ENISA should ensure that information about the notified vulnerability is shared in line with strict security protocols and on a need-to-know-basis***. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [Directive XXX / XXXX (NIS2)]. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised. In exceptional circumstances, at the request of the Commission, ENISA should be able to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.

Amendment 11

Proposal for a regulation
Recital 20

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

Amendment 12

Proposal for a regulation
Recital 22

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

these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.	change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.

Amendment 13

Proposal for a regulation
Recital 23

Text proposed by the Commission	*Amendment*
(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.	(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, ***the*** conformity assessment ***is updated***. 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. ***The subsequent conformity assessment should address the changes that lead to the new assessment, unless these changes have significant impact on the conformity of other parts of the product. Where software updates are implemented, the manufacturer should not be required to carry out another conformity assessment of the product with digital elements, unless the software update results in a substantial modification of the product with digital elements.***

Amendment 14

Proposal for a regulation
Recital 24 a (new)

Text proposed by the Commission	*Amendment*
	(24 a) Manufacturers of products with digital elements should ensure that software updates are provided in a clear and transparent way and clearly differentiate between security and functionality updates. Whilst security updates are designed to decrease the level of risk of a product with digital elements, the uptake of functionality updates provided by the manufacturer should always remain a user choice. Manufacturers should therefore provide these updates separately, unless technically unfeasible. Manufacturers should provide consumers with adequate information on the reasons behind each update and its foreseen impact on the product, as well as a clear and easy-to-use opt-out mechanism.

Amendment 15

Proposal for a regulation
Recital 25

Text proposed by the Commission	*Amendment*
(25) Products with digital elements should be considered critical if the negative impact of the exploitation of potential cybersecurity vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality, or the intended use. In particular, vulnerabilities in products with digital elements that have a cybersecurity-related functionality, such as secure elements, can lead to a propagation of security issues throughout the supply chain. The severity of the impact of a cybersecurity incident may also increase when taking into account the intended use of the product***, such as in an industrial setting*** or in the context of an	(25) Products with digital elements should be considered critical if the negative impact of the exploitation of potential cybersecurity vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality, or the intended use. In particular, vulnerabilities in products with digital elements that have a cybersecurity-related functionality, such as secure elements, can lead to a propagation of security issues throughout the supply chain. The severity of the impact of a cybersecurity incident may also increase when taking into account the intended use of the product ***in critical applications in sensitive environments,*** or

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.

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.

Amendment 16

Proposal for a regulation
Recital 26

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

Amendment 17

Proposal for a regulation
Recital 29

Text proposed by the Commission	*Amendment*
(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation[27] [the AI Regulation] which fall within the scope	(29) ***Products with digital elements or partly completed*** products with digital elements classified as high-risk AI systems according to Article 6 of Regulation [27] [the

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

[27] Regulation [the AI Regulation].

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 ***the [applicable provisions]*** of Regulation [the AI Regulation] should apply as a rule instead of the respective provisions of this Regulation. This rule should ***create a high*** level of assurance for critical products with digital elements covered by this Regulation. ***For*** 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 ***under*** this Regulation***, the responsible sectoral notified body should be responsible for conducting*** the conformity assessment ***under this*** Regulation ***and lead the administrative process such that economic operators can address their request for*** conformity assessment ***to a single regulatory body***.

[27] Regulation [the AI Regulation].

Amendment 18

Proposal for a regulation
Recital 32

Text proposed by the Commission	*Amendment*
(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***.	(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.

Amendment 19

Proposal for a regulation
Recital 33 a (new)

Text proposed by the Commission	*Amendment*
	(33 a) In order to ensure the products are designed, developed and manufactured in line with essential requirements foreseen in Section 1 of Annex I, manufacturers should exercise due diligence when integrating components sourced from third parties in products with digital elements. This is the case for components that are tailored to and integrated taken

	into account the specificities of the product, in particular in the case of free and open source software that have not been placed on the market in exchange of financial or other type of monetisation.

Amendment 20

Proposal for a regulation
Recital 34

Text proposed by the Commission	*Amendment*
(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of Directive [Directive XX/XXXX (NIS2)] are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database.	(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***, without undue delay and in any event within 48 hours of becoming aware of it, by means of an early warning,*** vulnerabilities that are being actively exploited***. Manufacturers should without undue delay of becoming aware of actively exploited vulnerability having a significant impact on the security of the product with digital elements further notify ENISA more details on the exploited vulnerability. All other vulnerabilities not having a significant impact on the security of the product with digital elements should be notified to ENISA once the vulnerability has been addressed***. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under

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

Amendment 21

Proposal for a regulation
Recital 34 a (new)

Text proposed by the Commission	*Amendment*
	(34 a) ENISA should be responsible for publishing and maintaining a database of known exploited vulnerabilities. Manufacturers should monitor the database and notify vulnerabilities found in their products.

Amendment 22

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(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	(35) Manufacturers should also report to ENISA***, by means of an early warning,*** any incident having ***a significant*** impact on the security of the product with digital elements***. Manufacturers should without undue delay and in any event within 72 hours of becoming aware of the significant incident related to the product with digital elements further notify ENISA more details on the significant incident***. 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

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.	elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having ***a significant*** impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident ***where appropriate and if likely to be adversely affected by it,*** and, where applicable, about ***risk mitigation and*** any corrective measures that the users can deploy to mitigate the impact of the ***significant*** 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. ***Without prejudice to other obligations, Manufacturers that identify vulnerability in a component integrated in a product with digital elements, including in a free and open source component, should report the vulnerability to the person or entity maintaining the component together with the corrective measure taken.***

Amendment 23

Proposal for a regulation
Recital 37 a (new)

Text proposed by the Commission	*Amendment*
	(37 a) According to the WTO Agreement on Technical Barriers to Trade, when technical regulations are necessary and relevant international standards exist, WTO Members should use those standards as the basis for their own technical regulations. It is important to avoid duplication of work among standardisation organizations, as international standards are intended to facilitate the harmonization of national and regional technical regulations and standards, thereby reducing non-tariff technical barriers to trade. Given that

cybersecurity is a global issue, the Union should strive for maximum alignment. To achieve this objective, the standardization request for this Regulation, as set out in Article 10 of Regulation 1025/2012, should seek to reduce barriers to the acceptance of standards by publishing their references in the Official Journal of the EU, in accordance with Article 10 (6) of Regulation 1025/2012.

Amendment 24

Proposal for a regulation
Recital 37 b (new)

Text proposed by the Commission	*Amendment*
	(37 b) Considering the broad scope of this Regulation, the timely development of harmonised standards poses a significant challenge. To enhance the security of products with digital components in the Union market as soon as possible, the Commission should be empowered for a limited time to declare existing international standards for cyber security of products as satisfying the requirements of this Regulation. These standards should be published as standards providing presumption of conformity.

Amendment 25

Proposal for a regulation
Recital 38

Text proposed by the Commission	*Amendment*
(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	(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[29] . 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.

[29] 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).

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[29] . Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements of this Regulation. ***The standardisation process should ensure a balanced representation of interests and effective participation of civil society stakeholders, including consumer organisations.***

[29] 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).

Amendment 26

Proposal for a regulation
Recital 41

Text proposed by the Commission	*Amendment*
(41) Where no harmonised standards ***are adopted or where the harmonised standards do not sufficiently address the essential*** requirements ***of this*** Regulation, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation	(41) Where no ***reference to*** harmonised standards ***covering the*** requirements ***set out in Annex I has been published in the Official Journal of the European Union in accordance with*** Regulation ***(EU) 1025/2012 and no such reference is expected to be published within a reasonable period***, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for

request by any of the European standardisation organisations, undue delays in the establishment of appropriate harmonised standards, or a lack of compliance of developed standards with the requirements of this Regulation or with a request of the Commission. In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.

developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation request by any of the European standardisation organisations, undue delays in the establishment of appropriate harmonised standards, or a lack of compliance of developed standards with the requirements of this Regulation or with a request of the Commission. In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.

Amendment 27

Proposal for a regulation
Recital 43

Text proposed by the Commission	*Amendment*
(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[30] . 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.	(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[30] . 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. ***However, a partly completed product with digital elements shall not be marked with the CE marking under this Regulation, without prejudice of marking provisions resulting from other applicable Union legislation.***

	For partly completed product with digital elements manufacturers should draw up an EU declaration of incorporation.
[30] 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).	[30] 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).

Amendment 28

Proposal for a regulation
Recital 45

Text proposed by the Commission	*Amendment*
(45) As a general rule the conformity assessment of products with digital elements should be carried out by the manufacturer under its own responsibility following the procedure based on Module A of Decision 768/2008/EC. The manufacturer should retain flexibility to choose a stricter conformity assessment procedure involving a third-party. If the product is classified as a critical product of class I, additional assurance is required to demonstrate conformity with the essential requirements set out in this Regulation. The manufacturer should apply harmonised standards, ***common specifications*** or cybersecurity certification schemes under Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act, if it wants to carry out the conformity assessment under its own responsibility (module A). If the manufacturer does not apply such harmonised standards, ***common specifications*** or cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party. Taking into account the administrative burden on manufacturers and the fact that cybersecurity plays an	(45) As a general rule ***the requirements for*** the conformity assessment of products with digital elements should ***be risk-based and to that regard in many cases the assessment could*** be carried out by the manufacturer under its own responsibility following the procedure based on Module A of Decision 768/2008/EC. The manufacturer should retain flexibility to choose a stricter conformity assessment procedure involving a third-party. If the product is classified as a critical product of class I, additional assurance is required to demonstrate conformity with the essential requirements set out in this Regulation. The manufacturer should apply harmonised standards, 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, 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

important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures respectively based on modules B+C or module H of Decision 768/2008/EC have been chosen as most appropriate for assessing the compliance of critical products with digital elements in a proportionate and effective manner. The manufacturer that carries out the third-party conformity assessment can choose the procedure that suits best its design and production process. Given the even greater cybersecurity risk linked with the use of products classified as critical class II products, the conformity assessment should always involve a third party.	cybersecurity plays an important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures respectively based on modules B+C or module H of Decision 768/2008/EC have been chosen as most appropriate for assessing the compliance of critical products with digital elements in a proportionate and effective manner. The manufacturer that carries out the third-party conformity assessment can choose the procedure that suits best its design and production process. Given the even greater cybersecurity risk linked with the use of products classified as critical class II products, the conformity assessment should always involve a third party.

Amendment 29

Proposal for a regulation
Recital 46 a (new)

Text proposed by the Commission	*Amendment*
	(46 a) Where products with digital elements are equivalent, one of these products can be accepted as representative of a family or category of products for purposes of certain conformity assessment procedures.

Amendment 30

Proposal for a regulation
Recital 55

Text proposed by the Commission	*Amendment*
(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	(55) In accordance with Regulation (EU) 2019/1020, market surveillance authorities carry out market surveillance in the territory of that Member State. This Regulation should not prevent Member States from choosing the competent

authorities to carry out those tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States may choose to designate any existing or new authority to act as market surveillance authority, including national competent authorities referred to in Article ***[Article X]*** of Directive ***[***Directive ***XXX/XXXX (NIS2)]*** or designated national cybersecurity certification authorities referred to in Article 58 of Regulation (EU) 2019/881. Economic operators should fully cooperate with market surveillance authorities and other competent authorities. Each Member State should inform the Commission and the other Member States of its market surveillance authorities and the areas of competence of each of those authorities and should ensure the necessary resources and skills to carry out the surveillance tasks relating to this Regulation. As per Article 10(2) and (3) of Regulation (EU) 2019/1020, each Member State should appoint a single liaison office that should be responsible, among others, for representing the coordinated position of the market surveillance authorities and assisting in the cooperation between market surveillance authorities in different Member States.	authorities to carry out those tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States may choose to designate any existing or new authority to act as market surveillance authority, including national competent authorities referred to in Article ***8*** of Directive ***(EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and*** Directive ***(EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive***) 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.

Amendment 31

Proposal for a regulation
Recital 56 a (new)

Text proposed by the Commission	*Amendment*
	(56 a) In order for economic operators that are SMEs and micro-businesses to be able to cope with the new obligations

imposed by this Regulation, the Commission should provide them with easy-to-understand guidelines and advice, for example, via a direct channel to connect to experts in case of questions, taking into account the need to simplify and limit the administrative burdens. When developing such guidelines, the Commission should take into consideration needs of SMEs so as to keep administrative and financial burdens to a minimum while facilitating their compliance with this Regulation. The Commission should consult relevant stakeholders, with expertise in the field of cybersecurity.

Amendment 32

Proposal for a regulation
Recital 58

Text proposed by the Commission	*Amendment*
(58) In certain cases, a product with digital elements which complies with this Regulation, may nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in ***[***Annex I to Directive ***XXX/XXXX (NIS2)]*** or to other aspects of public interest protection. Therefore it is necessary to establish rules which ensure mitigation of those risks. As a result, market surveillance authorities should take measures to require the economic operator to ensure that the product no longer presents that risk, to recall it or to withdraw it, depending on the risk. As soon as a market surveillance authority restricts or forbids the free movement of a product in such way, the	(58) In certain cases, a product with digital elements which complies with this Regulation, may nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in Annex I to Directive ***(EU) 2022/2555 (NIS2 Directive***) 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.

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.

Amendment 33

Proposal for a regulation
Recital 59

Text proposed by the Commission	*Amendment*
(59) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that these are not compliant with this Regulation, or for products that are compliant with this Regulation, but that present other important risks, such as risks to the health or safety of persons, fundamental rights or the provision of the services by essential entities of the type referred to in ***[***Annex I of Directive ***XXX / XXXX (NIS2)]***, the Commission may request ENISA to carry out an evaluation. Based on that evaluation, the Commission may adopt, through implementing acts, corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling of the respective	(59) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that these are not compliant with this Regulation, or for products that are compliant with this Regulation, but that present other important risks, such as risks to the health or safety of persons, fundamental rights or the provision of the services by essential entities of the type referred to in Annex I of Directive ***(EU) 2022/2555 (NIS2 Directive***), 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

products, within a reasonable period, commensurate with the nature of the risk. The Commission may have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the good functioning of the internal market, and only where no effective measures have been taken by surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities under the scope of ***[***Directive ***XXX / XXXX (NIS2)]***, while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the non-compliance with this Regulation or the important risks presented persist.

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 (NIS2 Directive***), while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the non-compliance with this Regulation or the important risks presented persist.

Amendment 34

Proposal for a regulation
Recital 62

Text proposed by the Commission	*Amendment*
(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	(62) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission in respect of updates to the list of critical products in Annex III and specifying the definitions of the these product categories. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of

protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential ***mandating of*** certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[33] . 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.

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

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 ***voluntary*** certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making [33] . 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.

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

Amendment 35

Proposal for a regulation
Recital 63

Text proposed by the Commission	*Amendment*
(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	(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[34] .	the type of information, format and procedure of the notifications on actively exploited vulnerabilities and incidents submitted to ENISA by the manufacturers***,*** ***based on industry best practices***, 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[34] .
[34] 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).	[34] 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).

Amendment 36

Proposal for a regulation
Recital 69

Text proposed by the Commission	*Amendment*
(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***	(69) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. This Regulation should apply [***36*** months] from

the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [12 months] from the entry into force of this Regulation.	its entry into force.

Amendment 37

Proposal for a regulation
Article 1 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
This Regulation lays down:	***The objective of this Regulation is to improve the functioning of the internal market while providing for a high level of consumer protection and cybersecurity.*** This Regulation lays down ***harmonised rules on***:

Amendment 38

Proposal for a regulation
Article 1 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) ***rules for*** the placing on the market of products with digital elements to ensure the cybersecurity of such products;	(a) the placing on the market of products with digital elements to ensure the cybersecurity of such products;

Amendment 39

Proposal for a regulation
Article 1 – paragraph 1 – point d

Text proposed by the Commission	*Amendment*
(d) ***rules on*** market surveillance and enforcement of the above-mentioned rules and requirements.	(d) market surveillance and enforcement of the above-mentioned rules and requirements.

Amendment 40

Proposal for a regulation
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. This Regulation applies to products with digital elements ***placed on the market*** whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to ***an external*** device or network.

Amendment 41

Proposal for a regulation
Article 2 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5 a. This Regulation does not apply to free and open-source software, including its source code and modified versions, unless the software is provided in the course of commercial activity, either by:
	(i) charging a price for a product;
	(ii) providing a software platform reliant on other services which the manufacturer monetises;
	(iii) using personal data generated by the software for reasons other than exclusively for improving the security, compatibility or interoperability of the software;
	(iv) charging a price for technical support services.
	The compliance of free and open-source components of products shall be ensured by the manufacturer of the product in which they are included.

Amendment 42

Proposal for a regulation
Article 2 – paragraph 5 b (new)

Text proposed by the Commission	*Amendment*
	5 b. This Regulation does not apply to the internal networks of a product with digital elements if these networks have dedicated endpoints and are completely isolated and secured from external data connection.

Amendment 43

Proposal for a regulation
Article 2 – paragraph 5 c (new)

Text proposed by the Commission	*Amendment*
	5 c. This Regulation shall not apply to spare parts intended solely to replace defective parts of products with digital elements, in order to restore their functionality.

Amendment 44

Proposal for a regulation
Article 3 – paragraph 1 – point 1

Text proposed by the Commission	*Amendment*
(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;	(1) 'product with digital elements' means any software or hardware product, including software or hardware components to be placed on the market separately;

Amendment 45

Proposal for a regulation
Article 3 – paragraph 1 – point 2

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

Amendment 46

Proposal for a regulation
Article 3 – paragraph 1 – point 6 a (new)

Text proposed by the Commission	*Amendment*
	(6 a) 'open-source software' means software distributed under a licence which allow users to run, copy, distribute, study, change and improve it freely, as well as to integrate it as a component in other products, provide it as a service, or provide commercial support for it;

Amendment 47

Proposal for a regulation
Article 3 – paragraph 1 – point 18

Text proposed by the Commission	*Amendment*
(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;	(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 ***its*** name or trademark, whether for payment or free of charge;

Amendment 48

Proposal for a regulation
Article 3 – paragraph 1 – point 19

Text proposed by the Commission	*Amendment*
(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;	(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 ***its*** behalf in relation to specified tasks ***with regard to the manufacturer's obligations***;

Amendment 49

Proposal for a regulation
Article 3 – paragraph 1 – point 23 a (new)

Text proposed by the Commission	*Amendment*
	(23 a) 'recall' means recall as defined in Article 3, point (22) of Regulation (EU) 2019/1020;

Amendment 50

Proposal for a regulation
Article 3 – paragraph 1 – point 26

Text proposed by the Commission	*Amendment*
(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;	***deleted***

Amendment 51

Proposal for a regulation
Article 3 – paragraph 1 – point 31

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

Amendment 52

Proposal for a regulation
Article 3 – paragraph 1 – point 39

Text proposed by the Commission	*Amendment*
(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;	(39) ‘actively exploited vulnerability’ means a ***patched*** 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;

Amendment 53

Proposal for a regulation
Article 3 – paragraph 1 – point 40 a (new)

Text proposed by the Commission	*Amendment*
	(40 a) 'partly completed products with digital elements' means a tangible item which is unable to function independently and which is only produced with the aim of be incorporated into or assembled with a product with digital elements or other partly completed product with digital elements, and which can only be effectively assessed for its conformity taking into account how it is incorporated into an intended final product with digital

elements;

Amendment 54

Proposal for a regulation
Article 3 – paragraph 1 – point 40 b (new)

Text proposed by the Commission	*Amendment*
	(40 b) 'life-cycle' means the period from the moment that product covered by this Regulation is placed on the market or put into service until the moment that it is discarded, including the effective time when it is capable of being used and the phases of transport, assembly, dismantling, disabling, scrapping or other physical or digital modifications foreseen by the manufacturer.

Amendment 55

Proposal for a regulation
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. Member States shall not impede, for the matters covered by this Regulation, the making available on the market of products with digital elements ***or partly completed products with digital elements*** which comply with this Regulation.

Amendment 56

Proposal for a regulation
Article 4 – paragraph 2

Text proposed by the Commission	*Amendment*
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	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.	***a prototype product with digital elements or a partly completed product with digital elements*** which does not comply with this Regulation ***provided that the product with digital elements is used exclusively for presentation purposes within the course of the event and that a visible sign clearly indicates its non-compliance with this Regulation***.

Amendment 57

Proposal for a regulation
Article 4 – paragraph 3

Text proposed by the Commission	*Amendment*
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.	3. Member States shall not prevent the making available of unfinished ***product with digital elements or a prototype product with digital elements*** which does not comply with this Regulation provided that ***it*** is only made available ***in a non-production version*** 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.

Amendment 58

Proposal for a regulation
Article 4 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3 a. This Regulation shall not prevent Member States from subjecting products with digital elements to additional measures when these specific products will be used for military, defence or national security purposes, in accordance with national and Union law, and such measures are necessary and proportionate for achievement of those purposes.

Amendment 59

Proposal for a regulation
Article 5 – paragraph 1 – point 1

Text proposed by the Commission	*Amendment*
(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	(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, ***provided with the necessary security updates***, and

Amendment 60

Proposal for a regulation
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products.	1. Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. ***Only*** products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products. ***Integrating a component of higher class of criticality into a product of lower criticality does not necessarily change the level of criticality for the product the component is integrated into.***

Amendment 61

Proposal for a regulation
Article 6 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(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)];	(b) the intended use ***in critical applications*** in sensitive environments, or by essential entities of the type referred to in the Annex [Annex I] to the Directive [Directive XXX/XXXX (NIS2)];

Amendment 62

Proposal for a regulation
Article 6 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) the intended use of performing critical or sensitive functions, such as processing of personal data;	(c) the intended use ***and scale*** of performing critical or sensitive functions, such as processing of personal data;

Amendment 63

Proposal for a regulation
Article 6 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Critical products with digital elements shall be subject to the conformity assessment procedures referred to in Article 24(2) and (3).	4. Critical products with digital elements shall be subject to the conformity assessment procedures referred to in Article 24(2) and (3). ***By exception, small and micro enterprises can use the procedure referred to in Article 24(2).***

Amendment 64

Proposal for a regulation
Article 6 – paragraph 5 – introductory part

Text proposed by the Commission	*Amendment*
5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical

products with digital elements for which the manufacturers ***shall be required to*** obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:

products with digital elements for which the manufacturers ***may*** obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:

Amendment 65

Proposal for a regulation
Article 8 – paragraph 1

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

Amendment 66

Proposal for a regulation
Article 8 – paragraph 2

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

Amendment 67

Proposal for a regulation
Article 8 – paragraph 3

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

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

Amendment 68

Proposal for a regulation
Article 9 – paragraph 1

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

Amendment 69

Proposal for a regulation
Article 10 – paragraph -1 (new)

Text proposed by the Commission	*Amendment*
	-1. Software manufacturers which qualify as a microenterprise as defined in Commission Recommendation 2003/361/EC shall make best efforts to comply with the requirements in this

	Regulation during the 6 months from placing a software on the market. This provision does not apply to highly critical products with digital elements.

Amendment 70

Proposal for a regulation
Article 10 – paragraph 1

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

Amendment 71

Proposal for a regulation
Article 10 – paragraph 4

Text proposed by the Commission	*Amendment*
4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. ***They shall*** ensure that such components do not compromise the security of the product with digital elements.	4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. ***It falls upon the manufacturer to*** ensure that such components do not compromise the security of the product with digital elements.

Amendment 72

Proposal for a regulation
Article 10 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4 a. The components manufacturers shall provide the information and

documentation necessary to comply with the requirements of this Regulation, when supplying such components to the manufacturer of finished products. This information shall be provided free of charge.

Amendment 73

Proposal for a regulation
Article 10 – paragraph 6 – subparagraph 1

Text proposed by the Commission	*Amendment*
When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is ***shorter***, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.	When placing a product with digital elements on the market, and for the expected product lifetime ***at the time of placing that product on the market*** or for a period of five years from the placing of the product on the market, whichever is ***longer***, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I***, provided that it is within the manufacturer's control***.

Amendment 74

Proposal for a regulation
Article 10 – paragraph 7 – subparagraph 3 a (new)

Text proposed by the Commission	*Amendment*
	Where software updates are implemented, the manufacturer shall not be required to carry out another conformity assessment of the product with digital elements, unless the software update results in a substantial modification of the product with digital elements within the meaning of Article 3(31) of this Regulation.

Amendment 75

Proposal for a regulation
Article 10 – paragraph 9

Text proposed by the Commission	*Amendment*
9. Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.	9. Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified. ***Where new knowledge, techniques, or standards become available, which were not available at the time of design of a serial product, the manufacturer may consider implementing such improvements periodically for future product generations.***

Amendment 76

Proposal for a regulation
Article 10 – paragraph 9 a (new)

Text proposed by the Commission	*Amendment*
	9 a. Manufacturers shall publicly communicate the expected product lifetime of their products, in a clear and understandable manner.

Amendment 77

Proposal for a regulation
Article 10 – paragraph 12

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

Amendment 78

Proposal for a regulation
Article 11 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The manufacturer shall, without undue delay and in any event within ***24*** hours of becoming aware of it, notify ***to*** ENISA any actively exploited vulnerability contained in the product with digital elements. ***The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability.***	1. The manufacturer shall, without undue delay and in any event within ***48*** hours of becoming aware of it, notify ENISA***, by means of an early warning, of*** any actively exploited vulnerability contained in the product with digital elements.

Amendment 79

Proposal for a regulation
Article 11 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1 a. The manufacturer shall without undue delay of becoming aware of actively exploited vulnerability having a significant impact on the security of the product with digital elements further notify ENISA more details on the exploited vulnerability.

Amendment 80

Proposal for a regulation
Article 11 – paragraph 1 b (new)

Text proposed by the Commission	*Amendment*
	1 b. All other vulnerabilities not having a significant impact on the security of the product with digital elements shall be notified to ENISA once the vulnerability has been addressed.

Amendment 81

Proposal for a regulation
Article 11 – paragraph 1 c (new)

Text proposed by the Commission	*Amendment*
	1 c. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken and the recommended risk mitigation measures. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of

	Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and immediately inform the market surveillance authority about the existence of a vulnerability and where applicable, the potential risk mitigation measures. Where a notified vulnerability has no corrective or mitigating measures available, ENISA shall ensure that information about the notified vulnerability is shared in line with strict security protocols and on a need-to-know-basis.

Amendment 82

Proposal for a regulation
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify ***to*** ENISA any incident having impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.	2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, ***by means of an early warning*** notify ENISA ***of*** any incident having ***a significant*** impact on the security of the product with digital elements***. The manufacturer shall without undue delay and in any event within 72 hours of becoming aware of the significant incident related to the product with digital elements further notify ENISA more details on the significant incident***. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and ***immediately*** inform the market surveillance authority about the notified ***significant*** incidents. The incident notification shall include information ***strictly necessary to make the competent authority aware of the incident, and where relevant and proportionate to the risk,*** 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. ***The mere act of notification shall not subject the notifying entity to increased liability.***

Amendment 83

Proposal for a regulation
Article 11 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. Economic operators that are also identified as essential entities or important entities under the NIS2 and who submit their incident notification pursuant to the NIS2 should be deemed compliant with the requirements in point 2 of this Article.

Amendment 84

Proposal for a regulation
Article 11 – paragraph 3

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

Amendment 85

Proposal for a regulation
Article 11 – paragraph 4

Text proposed by the Commission	*Amendment*
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.	4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the ***significant*** incident***, where appropriate and if likely to be adversely affected by it,*** and, where necessary, about ***risk mitigation and any*** corrective measures that the user can deploy to mitigate the impact of the ***significant*** incident ***concerning possible data affected and potential damage***.

Amendment 86

Proposal for a regulation
Article 11 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4 a. The obligations laid down in paragraphs 1, 2 and 4 will apply during the product lifetime. During the expected product lifetime period the manufacturer will provide security updates for free, which will apply only to products with digital elements for which the manufacturer has drawn up an EU declaration of conformity, in accordance with Article 20 of this Regulation.

Amendment 87

Proposal for a regulation
Article 11 – paragraph 5

Text proposed by the Commission	*Amendment*
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	5. The Commission***, after consulting stakeholders and CSIRTs,*** 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

the examination procedure referred to in Article 51(2).	acts shall ***take into account European and international standards and shall*** be adopted in accordance with the examination procedure referred to in Article 51(2).

Amendment 88

Proposal for a regulation
Article 11 – paragraph 6

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

Amendment 89

Proposal for a regulation
Article 11 – paragraph 7

Text proposed by the Commission	*Amendment*
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.	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 ***and the corrective or mitigating measure taken,*** to the person or entity maintaining the component. ***This does not release the manufacturer from the obligation to maintain the compliance of the product with the requirements of this regulation, nor does it create obligations for the developers of free and open source***

	components that have no contractual relation to the said manufacturer.

Amendment 90

Proposal for a regulation
Article 12 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
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:	3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. ***It shall provide a copy of the mandate to the market surveillance authorities upon request.*** The mandate shall allow the authorised representative to do at least the following:

Amendment 91

Proposal for a regulation
Article 12 – paragraph 3 – point a a (new)

Text proposed by the Commission	*Amendment*
	(a a) where the authorised representative has a reason to believe that a product with digital elements in question presents a cybersecurity risk, inform the manufacturer;

Amendment 92

Proposal for a regulation
Article 12 – paragraph 3 – point b

Text proposed by the Commission	*Amendment*
(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;	(b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the ***safety and the*** conformity of the product with digital elements ***in a***

	language which can be easily understood by that authority;

Amendment 93

Proposal for a regulation
Article 12 – paragraph 3 – point c

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

Amendment 94

Proposal for a regulation
Article 13 – paragraph 2 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) all the documents proving the fulfilment of the requirements set in this article have been received from the manufacturer and are available for inspection for a period of 10 years.

Amendment 95

Proposal for a regulation
Article 13 – paragraph 3

Text proposed by the Commission	*Amendment*
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	3. Where an importer considers or has reason to believe***, on the basis of the information at their disposal,*** 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

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.	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.

Amendment 96

Proposal for a regulation
Article 13 – paragraph 4

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

Amendment 97

Proposal for a regulation
Article 13 – paragraph 6 – subparagraph 1

Text proposed by the Commission	*Amendment*
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	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.	set out in Annex I, or to withdraw or recall the product, if appropriate. ***Based on a risk assessment, distributors and end users shall be timely informed of the lack of compliance and the risk mitigation measures they can take.***

Amendment 98

Proposal for a regulation
Article 14 – paragraph 2 – point b a (new)

Text proposed by the Commission	*Amendment*
	(b a) they have received from the manufacturer or the importer all the information and documentation required by this Regulation.

Amendment 99

Proposal for a regulation
Article 16 – paragraph 1

Text proposed by the Commission	*Amendment*
A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation.	A natural or legal person, other than the manufacturer, the importer or the distributor, that ***in the course of professional activity*** carries out a substantial modification of the product with digital elements ***and makes the product available on the market*** shall be considered a manufacturer for the purposes of this Regulation.

Amendment 100

Proposal for a regulation
Article 18 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1 a. The Commission shall, as provided in Article 10(1) of Regulation (EU)

1025/2012, request one or more European standardisation organisations to draft harmonised standards for the requirements set out in Annex I.

Amendment 101

Proposal for a regulation
Article 18 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4 a. In accordance with Article 10(1) of Regulation 1025/2012, when preparing the standardisation request for products within the scope of this Regulation, the Commission shall aim for maximum harmonisation with existing or imminent international standards for cybersecurity. In the first three years following the date of application of this Regulation, the Commission is empowered to declare an existing international standard as meeting the requirements of this Regulation, without any European modifications, provided that adherence to such standards sufficiently enhances the security of products with digital elements, and provided that the standard is published as a separate version by one of the European Standardisation Organisations.

Amendment 102

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
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***	***1.*** The Commission ***may adopt implementing acts establishing common specifications covering technical*** requirements ***that provide a means*** to comply with the ***essential health and safety requirements set out in Annex I for products within the scope of this***

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)***.	***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) 1025/2012; or
	(iii) the harmonised standards do not comply with the request; and
	(b) no reference to harmonised standards covering the requirements set out in Annex I has been published in the Official Journal of the European Union in accordance with Regulation (EU) 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 ***48(3)***.

Amendment 103

Proposal for a regulation
Article 19 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1 a. 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) 1025/2012 that it considers that the conditions in paragraph 3 have been fulfilled.

Amendment 104

Proposal for a regulation
Article 19 – paragraph 1 b (new)

Text proposed by the Commission	*Amendment*
	1 b. When preparing the draft implementing act referred to in paragraph 1, the Commission shall take into account the views of relevant bodies or the expert group and shall duly consult all relevant stakeholders.

Amendment 105

Proposal for a regulation
Article 19 – paragraph 1 c (new)

Text proposed by the Commission	*Amendment*
	1 c. 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) 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 1, or parts thereof which cover

the same requirements as those covered by that harmonised standard.

Amendment 106

Proposal for a regulation
Article 19 – paragraph 1 d (new)

Text proposed by the Commission	*Amendment*
	1 d. 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 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.

Amendment 107

Proposal for a regulation
Article 20 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	2. The EU declaration of conformity shall have the model structure set out in Annex IV and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VI. Such a declaration shall be updated ***as appropriate***. It shall be made available in ***a*** language ***which can easily be understood by the authorities of*** the Member State in which the product with digital elements is placed on the market or made available.

Amendment 108

Proposal for a regulation
Article 20 a (new)

Text proposed by the Commission	*Amendment*
	Article 20 a
	EU Declaration of Incorporation for partly completed products with digital elements
	1. The EU declaration of incorporation shall be drawn up by manufacturers in accordance with Article 10(7) and state that the fulfilment of the relevant essential requirements set out in Annex I has been demonstrated.
	2. The EU declaration of incorporation shall have the model structure set out in Annex IVa (new). Such a declaration shall be updated as appropriate. It shall be made available in the language or languages required by the Member State in which the partly completed product with digital elements is placed on the market or made available.
	3. Where a partly completed product with digital elements is subject to more than one Union act requiring an EU declaration of incorporation, a single EU declaration of incorporation 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. 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 incorporation as set out in Annex IVa (new) to take account of technological developments.

Amendment 109

Proposal for a regulation
Article 22 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 20 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product.	1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 20 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product. ***In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.***

Amendment 110

Proposal for a regulation
Article 22 – paragraph 3

Text proposed by the Commission	*Amendment*
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.	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 ***to consumers*** a special risk or use set out in implementing acts referred to in paragraph 6.

Amendment 111

Proposal for a regulation
Article 22 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE	5. Member States shall build upon existing mechanisms to ensure correct ***and harmonised*** application of the regime

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.	governing the CE marking and shall take appropriate ***and coordinated*** 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.

Amendment 112

Proposal for a regulation
Article 22 – paragraph 6

Text proposed by the Commission	*Amendment*
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)***.	6. The Commission may, by means of ***delegated*** acts, lay down technical specifications for ***labelling schemes, including harmonised labels,*** pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use ***among businesses and consumers and to increase public awareness about security of products with digital elements***. Those ***delegated*** acts shall be adopted in accordance with the procedure referred to in Article ***50***.

Amendment 113

Proposal for a regulation
Article 22 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6 a. A partly completed product with digital elements shall not be marked with the CE marking under this Regulation without prejudice of marking provisions resulting from other applicable Union legislation.

Amendment 114

Proposal for a regulation
Article 22 – paragraph 6 b (new)

Text proposed by the Commission	*Amendment*
	6 b. The Commission shall adopt guidelines and provide advice to economic operators, particularly those that qualify as SMEs, including micro-enterprises, on the implementation of this Regulation. In particular, the guidelines and the advice shall aim to simplify and limit the administrative and financial burdens, while ensuring the effective and consistent application of this Regulation in accordance with the general objective of ensuring product safety and consumer protection. The Commission should consult relevant stakeholders, with expertise in the field of cybersecurity.

Amendment 115

Proposal for a regulation
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
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***.	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 ***longer***.

Amendment 116

Proposal for a regulation
Article 23 – paragraph 3

Text proposed by the Commission	*Amendment*
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.	3. For products with digital elements 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.

Amendment 117

Proposal for a regulation
Article 23 – paragraph 5

Text proposed by the Commission	*Amendment*
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.	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by the elements to be included in the technical documentation set out in Annex V to take account of technological developments, as well as developments encountered in the implementation process of this Regulation. ***The Commission shall strive to minimise the administrative burden, especially for micro, small and medium sized enterprises.***

Amendment 118

Proposal for a regulation
Article 24 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) a European cybersecurity certification scheme adopted in accordance with Article 18(4) of Regulation (EU) 2019/881.

Amendment 119

Proposal for a regulation
Article 24 – paragraph 3 – point b

Text proposed by the Commission	*Amendment*
(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI**.**	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI***; or***

Amendment 120

Proposal for a regulation
Article 24 – paragraph 3 – point b a (new)

Text proposed by the Commission	*Amendment*
	(b a) where applicable, a European cybersecurity certification scheme at assurance level 'substantial' or 'high' pursuant to Regulation (EU) 2019/881.

Amendment 121

Proposal for a regulation
Article 24 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4 a. For products to which Union harmonisation legislation based on the New Legislative Framework apply, the manufacturer shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in Chapter III shall apply to those products.

Amendment 122

Proposal for a regulation
Article 24 – paragraph 5

Text proposed by the Commission	*Amendment*
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.	5. Notified bodies shall take into account the specific interests and needs of ***micro,*** small and medium sized enterprises when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs. ***The Commission shall take action to ensure more accessible and affordable procedures and appropriate financial support in the framework of existing Union programmes, particularly in order to ease the burden on micro, small and medium sized enterprises.***

Amendment 123

Proposal for a regulation
Article 24 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5 a. For products with digital elements falling within the scope of this Regulation and which are placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to 101 of that Directive.

Amendment 124

Proposal for a regulation
Article 24 a (new)

Text proposed by the Commission	*Amendment*
	Article 24 a
	Where products with digital elements have equivalent hardware or software, one product model can be representative of a family of products for the purposes of the following conformity assessment

	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.

Amendment 125

Proposal for a regulation
Article 27 – paragraph 5

Text proposed by the Commission	*Amendment*
5. A notifying authority shall safeguard the confidentiality of the information it obtains.	5. A notifying authority shall safeguard the confidentiality of the information ***including intellectual property rights, confidential business information and trade secrets*** it obtains.

Amendment 126

Proposal for a regulation
Article 27 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6 a. A notifying authority shall minimize bureaucracy and fees, especially for SMEs.

Amendment 127

Proposal for a regulation
Article 29 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7 a. Member States and the Commission shall put in place appropriate measures to ensure sufficient availability of skilled professionals, in order to

	minimise bottlenecks in the activities of conformity assessment bodies.

Amendment 128

Proposal for a regulation
Article 29 – paragraph 10

Text proposed by the Commission	*Amendment*
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.	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. ***Intellectual property*** rights***, confidential business information and trade secrets*** shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.

Amendment 129

Proposal for a regulation
Article 29 – paragraph 12

Text proposed by the Commission	*Amendment*
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.	12. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions ***in line with Article 37(2)***, in particular taking into account the interests of ***micro, small and medium sized enterprises*** in relation to fees.

Amendment 130

Proposal for a regulation
Article 36 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission shall ensure that all ***sensitive*** information obtained in the course of its investigations is treated confidentially.	3. The Commission shall ensure that all ***information, including intellectual property rights, confidential business*** information ***and trade secrets,*** obtained in the course of its investigations is treated confidentially.

Amendment 131

Proposal for a regulation
Article 37 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	2. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for economic operators***, with special consideration for SMEs***. Conformity assessment bodies shall perform their activities taking due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity ***and the risk exposure*** of the product ***type and*** technology in question and the mass or serial nature of the production process.

Amendment 132

Proposal for a regulation
Article 37 – paragraph 5

Text proposed by the Commission	*Amendment*
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	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 ***restrict,*** suspend or

the certificate if necessary.	withdraw the certificate if necessary.

Amendment 133

Proposal for a regulation
Article 40 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. The Commission shall ensure that appropriate coordination and cooperation between notified bodies are put in place ***taking also in account the need to reduce bureaucracy and fees,*** and properly operated in the form of a cross-sectoral group of notified bodies.

Amendment 134

Proposal for a regulation
Article 40 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	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***, taking also in account the need to reduce bureaucracy and fees***.

Amendment 135

Proposal for a regulation
Article 41 – paragraph 3

Text proposed by the Commission	*Amendment*
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	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.	implementation of the reporting obligations pursuant to Article 11 of this Regulation, the designated market surveillance authorities shall ***effectively*** cooperate with ENISA. ***The market surveillance authorities may request ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation, including during investigations in accordance with Article 43 when market surveillance authorities may request ENISA to provide non-binding evaluations of compliance of products with digital elements.***

Amendment 136

Proposal for a regulation
Article 41 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission shall facilitate the exchange of experience between designated market surveillance authorities.	7. The Commission shall facilitate the ***regular and structured*** exchange of experience between designated market surveillance authorities***, including via a dedicated administrative cooperation group (ADCO) established under paragraph 11 of this Article***.

Amendment 137

Proposal for a regulation
Article 41 – paragraph 8

Text proposed by the Commission	*Amendment*
8. ***Market surveillance authorities may*** provide ***guidance and*** advice to economic operators on the implementation of this Regulation, with the ***support of the Commission***.	8. ***The Commission shall adopt guidelines and*** provide advice to economic operators***, particularly those that qualify as SMEs, including micro-enterprises,*** on the implementation of this Regulation***. In particular***, ***the guidelines and the advice shall aim to simplify and limit the administrative and financial burden, while ensuring the effective and***

consistent application in accordance with the ***general objective of ensuring product safety and consumer protection***.

Amendment 138

Proposal for a regulation
Article 41 – paragraph 8 a (new)

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

Amendment 139

Proposal for a regulation
Article 41 – paragraph 11

Text proposed by the Commission	*Amendment*
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.	11. A dedicated administrative cooperation group (ADCO) shall be established for the uniform application of this Regulation, ***to facilitate structured cooperation in relation to the implementation of this Regulation and to streamline the practices of market surveillance authorities within the Union,*** pursuant to Article 30(2) of Regulation (EU) 2019/1020. This ADCO ***shall have, in particular, the tasks referred to in Article 32(2) of Regulation (EU) 2019/1020 and*** shall be composed of representatives of the designated market surveillance authorities***, ENISA*** and, if appropriate, representatives of single liaison offices. ***The ADCO shall meet at regular intervals and, where necessary, at the duly justified request of the***

	Commission or ENISA or a Member State and shall coordinate its action with other existing Union activities related to market surveillance and consumer safety and, where relevant, shall cooperate and exchange information with other Union networks, groups and bodies. The ADCO may invite experts and other third parties, including consumer organisations, to attend its meetings.

Amendment 140

Proposal for a regulation
Article 41 – paragraph 11 a (new)

Text proposed by the Commission	*Amendment*
	11 a. For products with digital elements falling within the scope of this Regulation, distributed, put into service or used by financial institutions regulated by relevant Union legislation on financial services, the market surveillance authority for the purposes of this Regulation shall be the relevant authority responsible for the financial supervision of those institutions under that legislation.

Amendment 141

Proposal for a regulation
Article 42 – paragraph 1

Text proposed by the Commission	*Amendment*
Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data required to assess the design, development, production and vulnerability handling of such products, including	Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data required to assess the design, development, production and vulnerability handling of such products, including

related internal documentation of the respective economic operator.	related internal documentation of the respective economic operator. ***Where appropriate, and in accordance with Article 52(1) point (a), this shall be in a secure, controlled environment determined by the manufacturer.***

Amendment 142

Proposal for a regulation
Article 43 – paragraph 1 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.	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 ***or otherwise presents a threat to national security***, it shall without delay require the relevant ***economic*** operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe. ***Before the above mentioned evaluation is conducted, if necessary, taking into account the significance of the cybersecurity risk, the market surveillance authority may require the relevant operator to immediately suspend or restrict the availability of the product on the market for the period of the above mentioned evaluation.***

Amendment 143

Proposal for a regulation
Article 43 – paragraph 4 – subparagraph 1

Text proposed by the Commission	*Amendment*
Where the manufacturer of a product with	Where the manufacturer of a product with

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

digital elements does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph***, or the relevant Member States authority consider product to present threat to the national security***, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it.

Amendment 144

Proposal for a regulation
Article 45 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it ***may*** request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.	1. Where the Commission has sufficient reasons to consider, including based on information provided by ***the competent authorities of Member States, the computer security incident response teams (CSIRTs) designated or established in accordance with Directive (EU) 2022/2555 or*** ENISA, that a product with digital elements that presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it ***shall*** request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.

Amendment 145

Proposal for a regulation
Article 45 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In ***exceptional*** circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission	2. In circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has reasons to

has ***sufficient*** reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***may*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***shall*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

Amendment 146

Proposal for a regulation
Article 46 – paragraph 1

Text proposed by the Commission	*Amendment*
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	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 ***(EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive***) or to other aspects of public interest protection, it shall require the relevant ***economic*** operator to take all appropriate measures to ensure that the

the risk.	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.

Amendment 147

Proposal for a regulation
Article 46 – paragraph 2

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

Amendment 148

Proposal for a regulation
Article 46 – paragraph 6

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

Amendment 149

Proposal for a regulation
Article 46 – paragraph 7

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

Amendment 150

Proposal for a regulation
Article 48 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Market surveillance authorities ***may agree*** with other relevant authorities ***to carry out joint activities*** aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks.	1. Market surveillance authorities ***shall regularly carry out joint activities*** with other relevant authorities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks. ***Those activities shall include inspections on products acquired under a cover identity.***

Amendment 151

Proposal for a regulation
Article 48 – paragraph 2

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

Amendment 152

Proposal for a regulation
Article 49 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. Market surveillance authorities ***shall regularly*** conduct simultaneous coordinated control actions (“sweeps”) of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation.

Amendment 153

Proposal for a regulation
Article 49 – paragraph 2

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

Amendment 154

Proposal for a regulation
Article 49 – paragraph 3

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

Amendment 155

Proposal for a regulation
Article 49 – paragraph 5

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

Amendment 156

Proposal for a regulation
Article 49 a (new)

Text proposed by the Commission	*Amendment*
	Article 49 a
	Provision of technical advice
	1. The Commission shall appoint by way of an implementing act an expert group to provide technical advice to market surveillance authorities on matters related to the implementation and enforcement of this Regulation. The implementing act shall specify, inter alia, the details related to the composition of

the group, its operation and the remuneration of its members. In particular, the expert group shall provide non-binding evaluations of products with digital elements upon request by a market surveillance authority that is conducting an investigation under Article 43 and of the list of critical products with digital elements set out in Annex II, as well as on the possible need to update that list.

2. The expert group shall consist of independent experts appointed for a renewable three-year term by the Commission on the basis of their scientific or technical expertise in the field.

3. The Commission shall appoint a number of experts which is deemed sufficient to fulfil the foreseen needs.

4. The Commission shall take the necessary measures to manage and prevent any conflicts of interest. The Declarations of interests of the members of the expert group shall be made publicly available.

5. The appointed experts shall perform their tasks with the highest level of professionalism, independence, impartiality and objectivity.

6. When adopting positions, views and reports, the expert group shall attempt to reach consensus. If consensus cannot be reached, decisions shall be taken by simple majority of the group members.

Amendment 157

Proposal for a regulation
Article 53 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall lay down the rules on penalties applicable to	1. Member States shall lay down the rules on penalties applicable to

infringements by economic operators of this Regulation and shall take all measures necessary to ensure that they are enforced. The penalties provided for shall be effective, proportionate and dissuasive.	infringements by economic operators of this Regulation and shall take all measures necessary to ensure that they are enforced. The penalties provided for shall be effective, proportionate and dissuasive ***and shall take into account the specificities of micro, small and medium sized enterprises***.

Amendment 158

Proposal for a regulation
Article 53 – paragraph 6 – point a a (new)

Text proposed by the Commission	*Amendment*
	(a a) whether the infringement is unintentional;

Amendment 159

Proposal for a regulation
Article 53 – paragraph 6 – point b

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

Amendment 160

Proposal for a regulation
Article 53 – paragraph 6 – point c

Text proposed by the Commission	*Amendment*
(c) the size and market share of the operator committing the infringement**.**	(c) the size and market share of the operator committing the infringement***, taking into account the scale of risks, consequences and financial specificities of micro, small and medium-sized enterprises;***

Amendment 161

Proposal for a regulation
Article 53 – paragraph 6 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) the subsequent behaviour of the operator following information or knowledge about the respective non-compliance, including whether upon becoming aware of the respective non-compliance the operator employed all the appropriate corrective measures as well as reasonably necessary measures to avoid or minimise potential negative consequences.

Amendment 162

Proposal for a regulation
Chapter VII a (new)

Text proposed by the Commission	*Amendment*
	MEASURES IN SUPPORT OF INNOVATION

Amendment 163

Proposal for a regulation
Article 53 a (new)

Text proposed by the Commission	*Amendment*
	Article 53 a
	Regulatory sandboxes
	The Commission and ENISA, may establish a European regulatory sandbox with voluntary participation of manufacturers of products with digital elements to:
	(a) provide for a controlled environment that facilitates the development, testing and validation of the design, development

and production of products with digital elements, before their placement on the market or putting into service pursuant to a specific plan;

(b) provide practical support to economic operators, including via guidelines and best practices to comply with the essential requirements set out in Annex I;

(c) contribute to evidence-based regulatory learning.

Amendment 164

Proposal for a regulation
Article 54 – title

Text proposed by the Commission	*Amendment*
Amendment to Regulation (EU) 2019/1020	Amendment to Regulation (EU) 2019/1020 ***and to Directive 2020/1828/EC***

Amendment 165

Proposal for a regulation
Article 54 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. In Annex I to Directive 2020/1828/EC the following point is added:
	'67. [Regulation XXX][Cyber Resilience Act].'

Amendment 166

Proposal for a regulation
Article 54 a (new)

Text proposed by the Commission	*Amendment*
	Article 54 a
	Delegated regulation (EU) 2022/30
	This Regulation is designed in such a way

	that all products covered by the essential requirements laid down in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU as described in the delegated regulation (EU) 2022/30 comply with this Regulation. To generate legal certainty the delegated regulation (EU) 2022/30 will be repealed when this Regulation comes into force.

Amendment 167

Proposal for a regulation
Article 57 – paragraph 2

Text proposed by the Commission	*Amendment*
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***]***.	It shall apply from [***36*** months after the date of entry into force of this Regulation]. ***As far as products with critical elements are concerned, Chapter II, III, V and VII*** shall apply ***no earlier than [20 months after the date of publication of the harmonised standards developed under the standardisation requires for the purpose of this Regulation].*** ***No later than 6*** months after the date of entry into force of this Regulation***, the Commission shall issue guidelines on how to apply the requirements in this Regulation to non-tangible products***.

Amendment 168

Proposal for a regulation
Annex I – Part 1 – point 3 – introductory part

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

Amendment 169

Proposal for a regulation
Annex I – Part 1 – point 3 – point - a (new)

Text proposed by the Commission	*Amendment*
	(-a) be placed on the market without any known exploitable vulnerabilities towards an external device or network;

Amendment 170

Proposal for a regulation
Annex I – Part 1 – point 3 – point a

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

Amendment 171

Proposal for a regulation
Annex I – Part 1 – point 3 – point c

Text proposed by the Commission	*Amendment*
(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;	(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by ***encryption, tokenization, compensating controls or other adequate protection of*** relevant data at rest or in transit by state of the art mechanisms;

Amendment 172

Proposal for a regulation
Annex I – Part 1 – point 3 – point d

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

Amendment 173

Proposal for a regulation
Annex I – Part 1 – point 3 – point f

Text proposed by the Commission	*Amendment*
(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	(f) protect the availability of essential ***and basic*** functions, including the resilience against and mitigation of denial of service attacks;

Amendment 174

Proposal for a regulation
Annex I – Part 1 – point 3 – point i

Text proposed by the Commission	*Amendment*
(i) be designed, developed and produced to reduce the impact of ***an*** incident using appropriate exploitation mitigation mechanisms and techniques;	(i) be designed, developed and produced to reduce the impact of ***a significant*** incident using appropriate exploitation mitigation mechanisms and techniques;

Amendment 175

Proposal for a regulation
Annex I – Part 1 – point 3 – point j

Text proposed by the Commission	*Amendment*
(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;	(j) provide security related information by ***providing at user request*** recording and/or monitoring ***capabilities, locally and at device level for*** relevant internal activity, including the access to or modification of data, services or functions;

Amendment 176

Proposal for a regulation
Annex I – Part 1 – point 3 – point k

Text proposed by the Commission	*Amendment*
(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users**.**	(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, ***separate from functionality updates and*** through automatic updates and the notification of available updates to users***;***

Amendment 177

Proposal for a regulation
Annex I – Part 1 – point 3 – point k a (new)

Text proposed by the Commission	*Amendment*
	(k a) be designed, developed and produced in order to allow for its secure discontinuation and potential recycling when reaching the end of the life cycle, including by allowing users to securely withdraw and remove all data on a permanent basis.

Amendment 178

Proposal for a regulation
Annex I – Part 2 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;	(2) in relation to the risks posed to the products with digital elements, address and remediate ***critical and high*** vulnerabilities without delay, including by providing security updates ***or document the reasons for not remediating the vulnerability***;

Amendment 179

Proposal for a regulation
Annex I – Part 2 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
(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 information helping users to remediate the vulnerabilities;	(4) once a security update has been made available, publically ***or according to industry best practice*** disclose information about fixed ***known*** vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and ***clear and accessible*** information helping users to remediate the vulnerabilities;

Amendment 180

Proposal for a regulation
Annex I – Part 2 – paragraph 1 – point 4 a (new)

Text proposed by the Commission	*Amendment*
	(4 a) information regarding fixes and vulnerabilities is shared and disclosed in a controlled way, respecting principles of 'harm reduction' and trade secrets through responsible disclosure of vulnerabilities to the actors who can act to mitigate the vulnerability, and that it is not made publicly available to avoid the risk of inadvertently informing potential attackers;

Amendment 181

Proposal for a regulation
Annex I – Part 2 – paragraph 1 – point 7

Text proposed by the Commission	*Amendment*
(7) provide for mechanisms to securely distribute updates for products with digital	(7) provide for mechanisms to securely distribute ***security*** updates for products

elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;	with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

Amendment 182

Proposal for a regulation
Annex I – Part 2 – paragraph 1 – point 8

Text proposed by the Commission	*Amendment*
(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.	(8) ensure that, where security patches or updates ***can reasonably be made*** available to address identified security issues, ***there is a means by which users can obtain them are disseminate*** without delay and free of charge ***or at a transparent and non-discriminatory cost***, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Amendment 183

Proposal for a regulation
Annex II – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
2. the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;	2. the ***single*** point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;

Amendment 184

Proposal for a regulation
Annex II – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
5. any known or foreseeable circumstance, related to the use of the product with digital elements in	***deleted***

accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;

Amendment 185

Proposal for a regulation
Annex II – paragraph 1 – point 6

Text proposed by the Commission	*Amendment*
6. if and, where applicable, where the software bill of materials can be accessed;	6. if and, where applicable, where the software bill of materials can be accessed ***by the competent authorities***;

Amendment 186

Proposal for a regulation
Annex II – paragraph 1 – point 8

Text proposed by the Commission	*Amendment*
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***;	8. the type of technical security support offered by the manufacturer and until when it will be provided;

Amendment 187

Proposal for a regulation
Annex II – paragraph 1 – point 8 a (new)

Text proposed by the Commission	*Amendment*
	8 a. the expected product lifetime end-date, clearly displaying, where applicable, on the packaging of the product, until when the manufacturer shall ensure the effective handling of vulnerabilities and provision of security updates;

Amendment 188

Proposal for a regulation
Annex II – paragraph 1 – point 9 – point a

Text proposed by the Commission	*Amendment*
(a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;	***deleted***

Amendment 189

Proposal for a regulation
Annex II – paragraph 1 – point 9 – point b

Text proposed by the Commission	*Amendment*
(b) how changes to the product can affect the security of data;	***deleted***

Amendment 190

Proposal for a regulation
Annex II – paragraph 1 – point 9 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) the expected product lifetime and until when the manufacturer ensures the effective handling of vulnerabilities and provision of security updates;

Amendment 191

Proposal for a regulation
Annex II – paragraph 1 – point 9 – point d

Text proposed by the Commission	*Amendment*
(d) the secure decommissioning of the product, including information on how user data can be securely removed.	***deleted***

Amendment 192

Proposal for a regulation
Annex III – Part I – point 3 a (new)

Text proposed by the Commission	*Amendment*
	3 a. Authentication, Authorization and Accounting (AAA) platforms;

Amendment 193

Proposal for a regulation
Annex III – Part I – point 15

Text proposed by the Commission	*Amendment*
15. Physical network interfaces;	15. Physical ***and virtual*** network interfaces;

Amendment 194

Proposal for a regulation
Annex III – Part I – point 18

Text proposed by the Commission	*Amendment*
18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;	***deleted***

Amendment 195

Proposal for a regulation
Annex III – Part I – point 23

Text proposed by the Commission	*Amendment*
23. Industrial Internet of Things not covered by class II.	23. Industrial ***products with digital elements that can be referred as part of*** Internet of Things not covered by class II.

Amendment 196

Proposal for a regulation
Annex III – Part II – point 4

Text proposed by the Commission	*Amendment*
4. Firewalls, intrusion detection and/or prevention systems intended for industrial use;	4. Firewalls***, security gateways***, intrusion detection and/or prevention systems intended for industrial use;

Amendment 197

Proposal for a regulation
Annex III – Part II – point 7

Text proposed by the Commission	*Amendment*
7. Routers, modems intended for the connection to the internet, ***and*** switches, ***intended for industrial use***;	7. Routers, modems intended for the connection to the internet, switches, ***and other network nodes that are necessary for the provision of the connectivity service***;

Amendment 198

Proposal for a regulation
Annex IV a (new)

Text proposed by the Commission	*Amendment*
	ANNEX IVa
	EU DECLARATION OF INCORPORATION FOR PARTLY COMPLETED PRODUCTS WITH DIGITAL ELEMENTS
	The EU declaration of incorporation for partly completed products with digital elements referred to in Article 20a, shall contain all of the following information:
	1. Name and type and any additional information enabling the unique identification of the partly completed product with digital elements;
	2. Object of the declaration (identification of the partly completed product allowing traceability. It may

	include a photograph, where appropriate);
	3. A statement that the partly completed product described above is in conformity with the relevant Union harmonisation legislation;
	4. References to any relevant Union acts concerned, including their publication references;
	5. Additional information:
	Signed for and on behalf of:
	……
	(place and date of issue):
	(name, function) (signature):

Amendment 199

Proposal for a regulation
Annex V – paragraph 1 – point 1 – point a

Text proposed by the Commission	*Amendment*
(a) its intended purpose;	***deleted***

Amendment 200

Proposal for a regulation
Annex V – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
2. a description of the design, development and production of the product and vulnerability handling processes, including:	***deleted***
(a) complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;	

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

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

Amendment 201

Proposal for a regulation
Annex V – paragraph 1 – point 3

Text proposed by the Commission	*Amendment*
3. ***an*** assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation;	3. ***a statement or a summary of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation and, further to a reasoned request from a market surveillance authority, provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I, a detailed*** assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation;

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

The following list is drawn up on a purely voluntary basis under the exclusive responsibility of the rapporteur. The rapporteur has received input from the following entities or persons in the preparation of the draft opinion:

Entity and/or person
Apple
BDI Federation of German Industries
BEUC
BSA The Software Alliance
Confederation of Danish Industries
Digital Europe
ETNO
Kaspersky
Microsoft
Samsung
TIC Council
Xiaomi

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
References	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)
Committee responsible Date announced in plenary	ITRE 9.11.2022
Opinion by Date announced in plenary	IMCO 9.11.2022
Associated committees - date announced in plenary	20.4.2023
Rapporteur for the opinion Date appointed	Morten Løkkegaard 16.12.2022
Discussed in committee	2.3.2023 25.4.2023 23.5.2023
Date adopted	29.6.2023
Result of final vote	+: 41 –: 1 0: 0
Members present for the final vote	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoş, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Alexandra Geese, Maria Grapini, Svenja Hahn, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Kateřina Konečná, Andrey Kovatchev, Maria-Manuel Leitão-Marques, Antonius Manders, Beata Mazurek, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann
Substitutes present for the final vote	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski
Substitutes under Rule 209(7) present for the final vote	Asger Christensen, Nicolás González Casares, Grzegorz Tobiszowski

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

41	+
ECR	Beata Mazurek, Grzegorz Tobiszowski, Kosma Złotowski
ID	Alessandra Basso, Marco Campomenosi, Virginie Joron
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Geoffroy Didier, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Asger Christensen, Svenja Hahn, Catharina Rinzema
S&D	Alex Agius Saliba, Biljana Borzan, Nicolás González Casares, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Tsvetelina Penkova, René Repasi, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Francisco Guerreiro, Kim Van Sparrentak

1	-
ECR	Eugen Jurzyca

0	0

Key to symbols:
+ : in favour
- : against
0 : abstention