European Parliament
2019-2024

Committee on Industry, Research and Energy

2022/0272(COD)

4.5.2023

AMENDMENTS
124 - 404

Draft report
Nicola Danti
(PE745.538v01-00)

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

Proposal for a regulation
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

AM_Com_LegReport

Amendment 124
Evžen Tošenovský

Proposal for a regulation
Title 1

Text proposed by the Commission	*Amendment*
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ***on horizontal*** cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ***on essential*** cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 ***(Cyber Resilience Act)*** (Text with EEA relevance)

Or. en

Amendment 125
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho, Lina Gálvez Muñoz

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) ***Cybersecurity is a key challenge for the European Union as the diffusion of products with digital elements is constantly rising. In this regard, cyberattacks are a matter of public interest as they can have a critical impact not only for the economy but also for consumers safety and health.*** It is ***therefore*** necessary to ***address cyber resilience at Union level and*** improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an

insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

Or. en

Amendment 126
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

Proposal for a regulation
Recital 4

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

market.	operators aiming at entering the Union market.

Or. en

Amendment 127
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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 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.	(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 products with digital elements ***connected to 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.

Or. en

Amendment 128
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

Proposal for a regulation
Recital 7 a (new)

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

Or. en

Amendment 129
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

Proposal for a regulation
Recital 7 b (new)

Text proposed by the Commission	*Amendment*
	(7b) 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.

Or. en

Amendment 130
Evžen Tošenovský

Proposal for a regulation
Recital 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) Directive (EU) 2022/2555 puts in place cybersecurity and incident reporting requirements for essential and important

entities, such as critical infrastructure, with a view to increasing the resilience of the services they provide. It applies to cloud computing services and cloud service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Network as a Service (NaaS). All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises and the smaller providers of cloud computing services identified in accordance with Article 2(2) fall in the scope of that Directive.

Or. en

Amendment 131
Ignazio Corrao
on behalf of the Verts/ALE Group

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	(9) This Regulation ensures a high level of cybersecurity of products with digital elements***, processes and ancillary*** services***. The definition and regulatory scope for products with digital elements should also include*** remote data processing solutions ***which are necessary for products*** with digital elements ***to perform its functions. Remote data processing solutions should be*** understood as any data processing at a distance***, irrespective of whether data is processed or stored locally on the device of the user or remotely. Moreover, manufacturers shall remain responsible*** for the software ***which*** is designed and developed***, as well as customised or substantially modified*** by the manufacturer of the product concerned or under the ***control or*** responsibility of that manufacturer, and the absence of which would prevent such a product with

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.

digital elements from performing one of its functions***. Software-as-a-Service (SaaS) shall constitute remote data processing solutions within the meaning of this Regulation to the extent that is inextricably linked to the performing one the product functions. For instance, websites or cloud service models supporting the functionality of products with digital elements fall in the scope of this Regulation***. [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. ***Where the manufacturer employs such cloud solutions which are not covered by NIS 2 or uses a custom implementation of a cloud service model, the requirements in this Regulation should be applicable.***

Or. en

Amendment 132
Evžen Tošenovský

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***	(9) This Regulation ***does not regulate the cloud computing services, it*** ensures a high level of cybersecurity of products with digital elements. ***The cloud enabled*** remote data processing solutions relating to a product with digital elements ***should be however considered as integral part of the product, only where the software for***

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.***

remote data processing is designed and developed by ***or for*** the manufacturer of the product concerned ***and is critical for the fundamental functions of the*** product with digital elements.

Or. en

Amendment 133
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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	(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 ***or on behalf of*** the manufacturer of the product concerned, and the absence of which would prevent such a product with digital elements from performing one of its ***essential*** functions. Directive ***(EU) 2022/2555 (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

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.	services they provide. Directive ***(EU) 2022/2555 (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.

Or. en

Justification

It should be clarified that only remote data processing solutions that are related to the product with digital elements should be considered to be in the scope of this Regulation.

Amendment 134
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 9 a (new)

Text proposed by the Commission	*Amendment*
	(9a) Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. Research by the European Commission also shows that free and open-source software can contribute between €65 billion to €95 billion to the European Union's GDP and that it can provide significant growth opportunities for the European economy. Users are allowed to run, copy, distribute, study, change and improve software and data, including models by way of free and open-source licences. To foster the development and deployment of free and open source software, especially by SMEs, start-ups, non-profits, academic research but also by individuals, this Regulation should not apply to such free and open-source software components, except in very

specific cases. We must take into account the fact that different development models of software distributed and developed under public licences exist, having a wide a range of different roles in such development models. For example commercial open-source exists and is generally developed by a single organisation or an asymmetric community, where a single organisation is generating significant revenues from related use in business relationships. In contrast, vendor-neutral free and open source is developed by a symmetric community, sometimes under the governance of a non-profit organisation, ensuring transparency and neutrality in the development model and with no direct revenues from related use in business relationships. This is why this Regulation should differentiate and the independent developers of free and open-source software components should not be mandated under this Regulation to comply with requirements targeting the product value chain and, in particular, not towards the manufacturer that has used that free and open-source software component in a commercial product. Developers of free and open-source software components, as well as all manufacturers that are not subject to stricter compliance rules, should however be encouraged to implement the provisions of Annex I, as a way to increase security, allowing the promotion of trustworthy products with digital elements in the EU.

Or. en

Amendment 135
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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) ***As a crucial tool for*** innovation ***and*** research, free and open-source software 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 by***:*** charging a price for a product***;*** charging a price for technical support services, ***when this does not serve only the recuperation of actual costs;*** providing a software platform through which the manufacturer monetises other services***;*** the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. ***The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity.*** ***When free and open-source software, supplied outside of the course of a commercial activity, is integrated into a final product with digital elements made available on the market, the economic operator that has placed the relevant product on the market shall be responsible for the compliance both of the product and of the integrated open-source software, according to this Regulation.***

Or. en

Amendment 136
Zdzisław Krasnodębski, Adam Bielan, Kosma Złotowski

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) 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. ***Nonetheless, 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 shall be required to make best efforts in order to comply with the requirements in this proposal during the 12 months from placing a software on the market. This special regime will prevent the chilling effect of high compliance and entry costs could have on entrepreneurs or skilled individuals who consider developing software in the European Union.***

Or. en

Amendment 137
Ignazio Corrao
on behalf of the Verts/ALE Group

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) ***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. As such, most package managers, code hosting, and collaboration platforms do not make*** software ***products available on the market as distributors within this Act.*** 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***, paid software updates***, by providing a software platform through which the ***provider*** monetises other services ***(such as an App Store)***, or by the use of ***data. Unrelated consulting services, membership fees and not for profit sponsorships do not constitute monetisation within the scope of this regulation.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 shall be responsible for the compliance of the product including of the free and open-source components***.

Or. en

Amendment 138
Bart Groothuis

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	(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***.***	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 ***solely occurs when*** a price ***is charged for the use of*** a product ***with the intention of making a profit beyond mere*** technical support***, consulting*** services, ***or maintenance based on incurred costs, or*** by providing a software platform through which the manufacturer ***monetises*** other services, or by the ***monetisation*** of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software

Or. en

Justification

Suggested language to clearly define commercial activity in the context of open-source software.

Amendment 139
Marc Botenga

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	(10) In order ***to enhance the collaborative development of free and open source software and*** not to hamper innovation or research, ***only*** free and open-source software ***used as a monetised product in*** a commercial activity should 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

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.	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. ***Under this Regulation, as manufacturer is considered the party commercially supplying the product to the market.***

Or. en

Amendment 140
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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) In order not to hamper innovation or research, ***only*** free and open-source software developed or supplied ***in*** 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 ***when this pursues a profit or the intention to monetise***, 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.

Or. en

Justification

Free and open-source software is defined by all users having access to the human-readable source code plus a license which grants permission to use, study, modify and share modified versions. This creates transparency and fosters both collaboration and competition, in turn making it a fundamental tool for innovation.

Amendment 141
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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) 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 ***solely occurs when*** a price ***is charged for the use of*** a product ***with the intention of making a profit or*** by providing a software platform through which the manufacturer monetises other services, or by the ***monetization*** of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

Or. en

Amendment 142
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

Proposal for a regulation
Recital 10 a (new)

Text proposed by the Commission	*Amendment*

(10a) The lack of professional skills in the field of cybersecurity is a key issue to be tackled for the succesful application of this Regulation. Therefore, in line with the European Commission Communication "Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy')", specific measures both at EU and Member States level should be put in place to assess the state and the evolution of cybersecurity labour market and create a single point of entry and synergies for cybersecurity education and training offers with the aim of establishing a common EU approach to cybersecurity training.

Or. en

Justification

As stated in the EC Communication "The Cybersecurity Skills Academy", in 2022 the shortage of cybersecurity professionals in the European Union ranged between 260.000 and 500.000.

Amendment 143
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

Proposal for a regulation
Recital 13 a (new)

Text proposed by the Commission	*Amendment*
	(13a) Agricultural and forestry vehicles in scope of Regulations (EU) 167/2013 of the European Parliament and of the Council fall also in the scope of this Regulation. In order to avoid regulatory overlaps, additional cybersecurity requirements in future amendments of Regulation (EU) 167/2013 should not be foreseen.

Or. en

Amendment 144
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) This Regulation should not apply to spare parts that are exclusively manufactured in order to repair and update products with digital elements that have been placed on the market before the application date of this Regulation.

Or. en

Amendment 145
Evžen Tošenovský

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 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	(19) ***CSIRTs*** should receive notifications from manufacturers of incidents having an impact on the security of those products. ***CSIRTs*** should also forward these notifications to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive ***(EU) 2022/2555***, and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive ***(EU) 2022/2555***. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able

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.***

to propose joint activities to be conducted by market surveillance authorities***, upon their request,*** 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.

Or. en

Amendment 146
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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	(19) Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer

Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in 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.	Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability***. ENISA should ensure the confidentiality of these notifications with particular regard to vulnerabilities for which a security update is not yet available***. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [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.

Or. en

Amendment 147
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Recital 19 a (new)

Text proposed by the Commission	*Amendment*
	(19a) ENISA should publish and maintain a known exploited vulnerability catalogue that should be included in the European vulnerability database established under Directive 2022/2555 (NIS2). The catalogue should assist manufacturers in detecting known exploitable vulnerabilities and notify vulnerabilities found in their products, in order to ensure that secure products are placed on the market.

Or. en

Amendment 148
Evžen Tošenovský

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***	(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, ***beyond necessary maintenance or security update,*** by physical or digital means, by the manufacturer and ***results in modification of the product's fundamental functions or its intended use and thus significantly affects*** the relevant essential requirements, the modification should be considered as substantial.

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

Or. en

Amendment 149
Nicola Danti

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 these changes were not foreseen in the initial risk assessment, or the nature of the	(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. ***Modifications to open source software aimed at fixing vulnerabilities or improving performance should not not be considered as substantial.*** 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

hazard has changed or the level of risk has increased because of 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.

Or. en

Amendment 150
Ignazio Corrao
on behalf of the Verts/ALE Group

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 these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has	(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 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

increased because of the software update.	assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.

Or. en

Amendment 151
Evžen Tošenovský

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, it is appropriate that the compliance of the product with digital elements is verified and that, where applicable, it undergoes ***an updated conformity assessment focusing on the modified elements or*** 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.

Or. en

Amendment 152
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 24 a (new)

Text proposed by the Commission	*Amendment*
	(24a) 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.

Or. en

Amendment 153
Marc Botenga

Proposal for a regulation
Recital 24 a (new)

Text proposed by the Commission	*Amendment*
	(24a) Manufacturers of products with digital elements shall provide software updates in a clear and transparent way in order to enhance the security protection and the functionality of the products, during the entire duration of the product's expected lifetime. Functionality and security updates shall be differentiated and users shall be clearly informed by the manufacturers regarding the nature and features of the updates. Software updates shall not intentionally affect the functionalities and the intended use of the products nor lessen its expected period of lifetime.

Or. en

Amendment 154

Ignazio Corrao
on behalf of the Verts/ALE Group

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 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***.	(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, the intended use ***or the size of market penetration of a particular product***. 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 ***or society***. The severity of the impact of a cybersecurity incident may also increase when taking into account the intended use of the product, such as in an industrial setting or in the context of an essential entity of the type referred to in Annex [Annex I] to Directive [Directive XXX/ XXXX (NIS2)], or for the performance of critical or sensitive functions, ***impacting health, safety or fundamental rights.***

Or. en

Amendment 155
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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	(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.	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. ***Periodical checks should be carried out to ensure that the list of critical products with digital elements is updated.***
	Or. en

Amendment 156
Marc Botenga

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 ***third-party*** conformity assessment procedures, ***certified by the relevant EU and Member States' authorities***. 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.
	Or. en

Amendment 157
Evžen Tošenovský

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 ***highly critical*** environments, and therefore should undergo a stricter conformity assessment procedure.

Or. en

Amendment 158
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) This Regulation addresses cybersecurity risks in a targeted manner. Products with digital elements might, however, pose other safety risks, that are not related to cybersecurity. Those risks should continue to be regulated by other relevant Union product legislation. If no other Union harmonisation legislation is applicable, they should be subject to Regulation [General Product Safety Regulation]. Therefore, in light of the	(28) This Regulation addresses cybersecurity risks in a targeted manner. Products with digital elements might, however, pose other safety risks, that are not ***always*** related to cybersecurity ***but can be a consequence of a security breach***. Those risks should continue to be regulated by other relevant Union product legislation ***as a rule if a higher level of protection is conferred. If not, safety risks in connection with the cybersecurity***

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

functions of products with digital elements should fall within the scope of this Regulation. If no other Union harmonisation legislation is applicable, they should be subject to Regulation [General Product Safety Regulation]. Therefore, in light of the targeted nature of this Regulation, as a derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] should apply to products with digital elements with respect to safety risks not covered by this Regulation, if those products are not subject to specific requirements imposed by other Union harmonisation legislation within the meaning of [Article 3, point (25) of the General Product Safety Regulation].

Or. en

Amendment 159
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 30

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

requirements is demonstrated by the EU declaration of conformity issued under this Regulation.

Or. en

Amendment 160
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 31

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

Or. en

Amendment 161
Evžen Tošenovský

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, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product***, they should for instance ensure that all their products are delivered without any known patched vulnerabilities or that the appropriate impact mitigation such as by security updates before the product is put into service for the first time***. 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 ***or international*** standards.

Or. en

Amendment 162
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Angelika Niebler

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	(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.	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 exploitable vulnerabilities ***known to them***, 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.

Or. en

Amendment 163
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 32 a (new)

Text proposed by the Commission	*Amendment*
	(32a) In order to ensure the products are designed, developed and produced 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. Given that such components 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, the

manufacturer of the product shall be responsible for ensuring its compliance.

Or. en

Amendment 164
Evžen Tošenovský

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 ***(EU) 2022/2555*** are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ***CSIRTs all fixed*** vulnerabilities***, and on a voluntary basis also unpatched vulnerabilities***. 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 ***therefore disclose*** fixed vulnerabilities to the European vulnerability database established under Directive ***(EU) 2022/2555*** and managed by ENISA***. Manufacturers should also benefit from coordinated*** vulnerability ***disclosure mechanism established under Directive (EU) 2022/2555***.

Or. en

Amendment 165
Bart Groothuis

Proposal for a regulation
Recital 34 a (new)

Text proposed by the Commission	*Amendment*
	(34a) Dependencies on high-risk suppliers of critical products with digital elements intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)] pose a strategic risk that needs to be mitigated at Union level. To mitigate this strategic risk there is a need to move beyond non-binding initiatives, such as the 5G toolbox, and move towards a binding toolbox for reducing critical ICT supply chain risks adopted as a delegated act. It should leverage the lessons learned from those past and national experiences, be based upon a risk assessment and offer strategic risk mitigation measures. Critical products with digital elements used in critical sectors should therefore be subjected to a strategic supply chain risk assessment that includes non-technical factors to assess the risk of the manufacturer being subject to undue interference from a third country. Those factors may include the jurisdiction of the supplier/manufacturer and the characteristics of the supplier's corporate ownership and the links of control to a third-country government where it is established. A high risk is attributed to a third country's legislation that obliges arbitrary access to any kind of company data, that would e.g. allow it to conduct economic espionage, without legislative or democratic checks and balances, meaningful oversight mechanisms or the right to appeal to an independent judiciary. A high risk is also attributed where a manufacturer is operating under foreign ownership or control that has the power, direct or indirect, whether or not exercised, to direct or decide matters affecting the management or operations of the manufacturer, or in case of opaque ownership structures, which are are state-owned or controlled. Not all instances of

control will create security risks, but what should be considered is the extent to which the use of the critical product by the entities: (a) includes access to sensitive or classified information or assets, (b) relates to the storage or transport of sensitive materials or substances, (c) relates to the provision of security services for physical sites or facilities, (d) is for, or relates to, the storage or protection of sensitive or classified information. Non-technical risk factors should not impede procurement from entities established in likeminded strategic partner countries.

Or. en

Justification

The CRA has a missed opportunity to not address the issue of risky vendors, especially in the context of critical infrastructure. While there have been positive developments towards non-binding toolboxes to address specific supply chain security issues related 5G (toolbox) the European Court of Auditors concluded that since the 5G toolbox was adopted, progress has been made to reinforce the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors, but that none of the measures put forward are legally binding, meaning that implementation across the Union is inconsistent at best, and that the Commission has no power to enforce those rules. This should be addressed in the Cyber Resilience Act.

Amendment 166
Ignazio Corrao
on behalf of the Verts/ALE Group

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	(35) Manufacturers should also report to ENISA any incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive [Directive XXX/XXXX (NIS2)] for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in

accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.	accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly. ***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, and provide the corresponding code under a free and open source licence.***
	Or. en

Amendment 167
Evžen Tošenovský

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	(35) Manufacturers should also report to ***CSIRTs any significant*** incident having an impact on the security of the product with digital elements***, and on a voluntary basis any other incident, near miss or cyber threat***. Notwithstanding the incident reporting obligations in Directive ***(EU) 2022/2555*** for essential and important

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

entities, it is crucial for ***CSIRT,*** ENISA, the single points of contact designated in accordance with Article ***8*** of Directive ***(EU) 2022/2555*** and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.

Or. en

Amendment 168
Evžen Tošenovský

Proposal for a regulation
Recital 35 a (new)

Text proposed by the Commission	*Amendment*
	(35a) The manufacturers of products with digital elements are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under this Regulation, Directive (EU) 2022/2555,

and possibly also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. The Commission should develop and adopt common notification templates by means of implementing acts that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.

Or. en

Amendment 169
Angelika Niebler

Proposal for a regulation
Recital 35 a (new)

Text proposed by the Commission	*Amendment*
	(35a) To minimise bureaucratic burden, especially on SMEs, there should be only two reporting stages after discovering an actively exploited vulnerability and the reportings should include only necessary information to make the competent authority aware of the incident and the measures taken and allow for the entity to seek assistance. The early warning after 24 hours should be seen as first notification with only the most essential information to raise ENISA's awareness of the incident. After 72 hours, a manufacturer should state more precisely which measures were taken after the incident.

Or. en

Amendment 170
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Angelika Niebler

Proposal for a regulation
Recital 35 a (new)

Text proposed by the Commission	*Amendment*
	(35a) Reporting should be as convenient and efficient as possible. For this purpose, ENISA should provide for an online system into which all requested information can be inserted.

Or. en

Amendment 171
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

Proposal for a regulation
Recital 36

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

Or. en

Amendment 172
Evžen Tošenovský

Proposal for a regulation
Recital 36

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

Or. en

Amendment 173
Evžen Tošenovský

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(37) In order to facilitate vulnerability	(37) In order to facilitate vulnerability

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

Or. en

Amendment 174
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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 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.	(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 ***horizontal or domain specific*** 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	[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).

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).

Or. en

Amendment 175
Evžen Tošenovský, Adam Bielan

Proposal for a regulation
Recital 38 a (new)

Text proposed by the Commission	*Amendment*
	(38a) 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 organisations, as international standards are intended to facilitate the harmonisation of national and regional technical regulations and standards, thereby reducing non-tariff technical barriers to trade. Given that cybersecurity is a global issue, the EU should strive for maximum alignment. To achieve this objective, the standardisation request for this Regulation, as set out in Article 10 of Regulation (EU) 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 (EU) 1025/2012.

Or. en

Amendment 176
Evžen Tošenovský, Adam Bielan

Proposal for a regulation
Recital 38 b (new)

Text proposed by the Commission	*Amendment*
	(38b) 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, international standards should be published as a standard providing presumption of conformity.

Or. en

Amendment 177
Christophe Grudler, Valérie Hayer

Proposal for a regulation
Recital 39

Text proposed by the Commission	*Amendment*
(39) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, processes and services. European cybersecurity certification schemes ***can cover*** products ***with digital elements covered by this Regulation***. This Regulation should create synergies with Regulation (EU) 2019/881. In order to facilitate the assessment of conformity with the requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and which has been identified by the Commission in an	(39) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, processes and services. European cybersecurity certification schemes ***thus provide a common framework of trust for users to use ICT*** products ***by assessing their level of cybersecurity***. This Regulation should ***consequently*** create synergies with Regulation (EU) 2019/881***. Regulation (EU) 2019/881 should address products with critical cybersecurity aspects and this Regulation should be dedicated to minimising the risk of incidents and cyberattacks***. In order to facilitate the assessment of conformity with the

implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity certification schemes for products with digital elements should be assessed in the light of this Regulation. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation. The Commission should be empowered to specify, by means of implementing acts, the European cybersecurity certification schemes ***that can be used*** to demonstrate conformity with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, ***where applicable, the Commission*** should ***specify if a cybersecurity certificate issued under such European cybersecurity certification schemes eliminates the*** obligation ***for*** manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements.

requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and which has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity certification schemes for products with digital elements should be assessed in the light of this Regulation. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation. The Commission should be empowered to specify, by means of implementing acts, the ***use of*** European cybersecurity certification schemes ***for critical products*** to demonstrate conformity with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, ***there*** should ***be no*** obligation ***on*** manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements ***where a cybersecurity certificate has been issued under such European cybersecurity certification schemes, at a substantial or high level***.

Or. en

Justification

The CRA should be better linked to the Cyber Security Act (CSA) in order to avoid overlaps between the two texts. As the CSA lays down a more rigorous cybersecurity assessment framework, it should address products presenting a particular cybersecurity risk. As the conformity assessment framework specific to the CRA is less demanding, it should be used to address mass products subjected to the CRA.

Amendment 178
Evžen Tošenovský, Adam Bielan

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 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.	***deleted***

Or. en

Amendment 179
Massimiliano Salini

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 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.	(41) Where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation request by any of the European standardisation organisations, undue delays in the establishment of appropriate harmonised standards, or a lack of compliance of developed standards with the requirements of this Regulation or with a request of the Commission. ***When developing such common specifications, the Commission should take into consideration the relevant international standards.*** 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.

Or. en

Justification

When adopting the common specifications, the Commission should refer to the already existing international standards that are mainly used in the market, instead of developing new ones.

Amendment 180
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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

Or. en

Amendment 181
Ignazio Corrao
on behalf of the Verts/ALE Group

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	(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

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

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

Or. en

Amendment 182

Evžen Tošenovský, Adam Bielan

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 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	(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, ***international 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, ***international 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 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.	cybersecurity risk linked with the use of products classified as critical class II products, the conformity assessment should always involve a third party.

Or. en

Amendment 183
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

Proposal for a regulation
Recital 53

Text proposed by the Commission	*Amendment*
(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.	(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators***, in particular for micro, small, medium sized enterprises. In this regard, Member States, with the support of the Commission, should ensure that there is an adequate availability of cybersecurity skilled professionals in order to ensure that notified bodies can carry out their activities efficiently thus facilitating economic operators' compliance to this Regulation***. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.

Or. en

Amendment 184
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Recital 53

Text proposed by the Commission	*Amendment*
(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden ***for*** economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.	(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden ***on*** economic operators***. In order to ensure that notified bodies are able to perform their tasks efficiently, and to minimise possible impediments, the Commission and Member States should ensure that there are skilled professionals in the Union***. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.

Or. en

Amendment 185
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Recital 53 a (new)

Text proposed by the Commission	*Amendment*
	(53a) In order to increase efficiency and transparency, the Commission should within 24 months from the entry into force of this Regulation, ensure that there is a sufficient number of notified bodies in the Union to carry out a conformity assessment, in order to avoid bottlenecks and hindrances to market entry.

Or. en

Amendment 186
Evžen Tošenovský

Proposal for a regulation
Recital 56

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

Or. en

Amendment 187
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation
Recital 57 a (new)

Text proposed by the Commission	*Amendment*
	(57a) In this framework, in order to provide updated information on the cyber security of critical products with digital elements, as defined in Annex III, the Commission should consider the adoption of measures aimed at informing the

market on products that, according to Article 10 (6) of this Regulation, will not receive any further cyber security management.

Or. en

Amendment 188
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation
Recital 61

Text proposed by the Commission	*Amendment*
(61) Simultaneous coordinated control actions (‘sweeps’) are specific enforcement actions by market surveillance authorities that can further enhance product security. Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps could be organised to the market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives.	(61) Simultaneous coordinated control actions (‘sweeps’) are specific enforcement actions by market surveillance authorities that can further enhance product security. Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps could be organised to the market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives. ***ENISA should also coordinate national market surveillance authorities for regular checks of products with digital elements placed on the market by manufacturers that might present a security risk for the EU, with particular regard to identifying exploitable vulnerabilities.***

Or. en

Amendment 189
Beatrice Covassi

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 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.	(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. ***Powers to adopt acts should also be delegated to 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 manufacturers. The Commission is also empowered to adopt delegated acts to establish common specifications in respect of the essential requirements set out in Annex I.*** It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[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.

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

Or. en

Amendment 190
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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 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	(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***. Such updates shall be carried out periodically by the Commission, ensuring timely changes to the list of critical products in Annex III***. 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

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.

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.

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

Or. en

Amendment 191
Beatrice Covassi, Robert Hajšel, Patrizia Toia

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 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	(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to: specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts therefore as set out in Annex I of this Regulation, lay down technical specifications for pictograms or any other marks related to

(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 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).

Or. en

Amendment 192
Bart Groothuis

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 the type of information, format and procedure of the notifications on actively exploited vulnerabilities and incidents	(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to***, in open consultation with stakeholders and in consideration of international and industry standards***: specify the format and elements of the software bill of materials, specify further the type of information,

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].

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].

[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).

Or. en

Amendment 193
Evžen Tošenovský

Proposal for a regulation
Recital 63

Text proposed by the Commission

(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should

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 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].	be conferred on the Commission to: specify the ***recommended*** format and elements of the software bill of materials, specify further the type of information, format and procedure of the notifications on ***patched*** vulnerabilities and incidents submitted to ***CSIRTs*** 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, 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).

Or. en

Amendment 194
Evžen Tošenovský

Proposal for a regulation
Recital 65

Text proposed by the Commission	*Amendment*

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

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

Or. en

Amendment 195
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

Proposal for a regulation
Recital 65

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

Or. en

Amendment 196
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

Proposal for a regulation
Recital 66 a (new)

Text proposed by the Commission	*Amendment*
	(66a) The revenues generated from the payments of penalties should be used to strengthen the level of cybersecurity within the Union, including by developing capacity and skills related to cybersecurity, improving economic operators' cyber resilience, in particular of micro, small and medium sized enterprises and more in general fostering public awareness of cyber security issues.

Or. en

Amendment 197
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Or. en

Amendment 198

Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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 the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [12 months] from the entry into force of this Regulation.	(69) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. This Regulation should apply [***30*** months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [12 months] from the entry into force of this Regulation.

Or. en

Amendment 199
Evžen Tošenovský

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 the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [***12*** months] from the entry into force of this Regulation.	(69) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. This Regulation should apply [***60*** months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [***24*** months] from the entry into force of this Regulation.

Or. en

Amendment 200
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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 the reporting obligations concerning ***actively*** exploited vulnerabilities and incidents, which should apply [***12*** months] from the entry into force of this Regulation.	(69) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. This Regulation should apply [***32*** months] from its entry into force, with the exception of the reporting obligations concerning ***known*** exploited vulnerabilities and incidents, which should apply [***22*** months] from the entry into force of this Regulation.

Or. en

Justification

The implementation period of this Regulation should be extended to 32 months in order to give economic operators, notified bodies and enforcement authorities sufficient time to adapt to new methodologies introduced by the Regulation.

Amendment 201
Evžen Tošenovský, Adam Bielan

Proposal for a regulation
Recital 69 a (new)

Text proposed by the Commission	*Amendment*
	(69a) Economic operators that are SMEs, with particular attention paid to micro enterprises and start-ups, should be provided with dedicated guidance and where possible with financial support to adapt to the requirements of this Regulation when placing new product on the market. In particular, the Commission, ENISA and the Member States, should establish a European cyber resilience regulatory sandboxes, the Commission should establish a special webpage and provide direct tailored advice, and streamline the financial support from Digital Europe Programme and other relevant EU programmes. Member States should consider all possible complementary actions aiming at

advice and financial support for SMEs, including via digital/cybersecurity hubs and start-up accelerators. Where the market surveillance authorities exercise their supervisory enforcement tasks, they should take into consideration whether the manufacturer is a SME, with particular attention payed to micro companies and start-ups.

Or. en

Amendment 202
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Recital 69 a (new)

Text proposed by the Commission	*Amendment*
	(69a) This Regulation may generate additional costs to micro, small and medium-sized enterprises. In order to support these enterprises that may face additional costs, the Commission should establish financial and technical support that allows for these companies to contribute to the European cybersecurity landscape.

Or. en

Amendment 203
Christophe Grudler, Valérie Hayer

Proposal for a regulation
Recital 70 a (new)

Text proposed by the Commission	*Amendment*
	(70a) This Regulation is without prejudice to the Member States' prerogatives to take measures safeguarding national security, in compliance with Union law. Member States should be able to apply additional

measures to products with digital elements that are used for military, defence or national security purposes.

Or. en

Justification

The maximal harmonisation nature of the regulation does not allow Member States to apply additional national requirements for regulated products, given that such additional requirements could prevent products that do not meet these additional requirements from accessing the market. It is important to preserve this ability of Member States to apply additional requirements for very specific use-cases and products with higher cybersecurity risks, in particular when national security is involved.

Amendment 204
Ignazio Corrao
on behalf of the Verts/ALE Group

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) rules on ***market monitoring,*** market surveillance and enforcement of the above-mentioned rules and requirements.

Or. en

Amendment 205
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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) rules on market ***monitoring,*** surveillance and enforcement of the above-mentioned rules and requirements.

Or. en

Amendment 206
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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 whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to ***an external*** device or network. ***This Regulation does not apply to the electronic communications networks as defined in Article 2, point (1), of Directive (EU) 2018/1972 in which products with digital elements are integrated.***

Or. en

Amendment 207
Evžen Tošenovský

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 a device or network.

Or. en

Amendment 208
Beatrice Covassi, Robert Hajšel, Patrizia Toia

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 ***that have*** a direct or indirect logical or physical data connection to ***an external*** device or network.

Or. en

Amendment 209
Bart Groothuis

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 whose intended use includes a direct or indirect logical or physical data connection to a device or network.

Or. en

Justification

The reasonably foreseeable use cannot always be forecasted always by the manufacturer.

Amendment 210
Evžen Tošenovský, Adam Bielan

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

Text proposed by the Commission	*Amendment*
	(ca) Regulation (EU) 2022/2554.

Or. en

Amendment 211
Massimiliano Salini

Proposal for a regulation
Article 2 – paragraph 3

Text proposed by the Commission	*Amendment*
3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.	3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139***, nor to products with digital elements that are isolated from external devices and networks***.

Or. en

Justification

The Regulation should not address products with digital elements used only for internal functioning and not interacting externally.

Amendment 212
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 2 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. This Regulation shall not apply to software provided under free and open-source licences, including its source code and modified versions, except when such software is provided as a paid or monetised product. The compliance of free and open-source components of products shall be ensured by the manufacturer of the product.

Or. en

Amendment 213
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation

Article 2 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. This regulation does not apply to spare parts that are exclusively manufactured in order to repair products with digital elements that have been placed on the market before the application date of this regulation referred to in Article 57.

Or. en

Amendment 214
Christophe Grudler, Valérie Hayer

Proposal for a regulation
Article 2 – paragraph 5

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

Or. en

Justification

Aligned with NIS2

Amendment 215
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	5a. This Regulation does not apply to any supply of a product with digital elements for distribution and use on the Union market where such supply,

distribution, and use exclusively occurs within the same group of companies within the meaning of Article 2(13) of Regulation (EU) 2015/848.

Or. en

Amendment 216
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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

Text proposed by the Commission	*Amendment*
	5a. This Regulation does not apply to free and open-source software, including its source code and modified versions, except when such software is provided in exchange for a price or as a monetised product with the intention of making a profit rather than performing maintenance.

Or. en

Amendment 217
Marc Botenga

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

Text proposed by the Commission	*Amendment*
	5a. This regulation does not apply to free and open source software supplied outside the course of a commercial activity.

Or. en

Amendment 218
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi,

Markus Buchheit, Marie Dauchy

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

Text proposed by the Commission	*Amendment*
	5b. 6 (new) This Regulation does not apply to the internal networks of a product with digital elements if these networks have dedicated endpoints and are secured from external data connection.

Or. en

Amendment 219
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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

Text proposed by the Commission	*Amendment*
	5c. 7 (new) 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.

Or. en

Amendment 220
Ignazio Corrao
on behalf of the Verts/ALE Group

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	(1) 'product with digital elements' means any software or hardware product its ***ancillary services, including*** remote data processing solutions, ***and*** software or

components to be placed on the market separately;	hardware components to be placed on the market separately;

Or. en

Amendment 221
Evžen Tošenovský

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;

Or. en

Amendment 222
Bart Groothuis

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;

Or. en

Justification

To avoid overlap with NIS2 (remote data processing).

Amendment 223

Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	(1a) 'consumer product with digital elements' means any product with digital elements' to be placed on the market with default generic security configuration;

Or. en

Amendment 224
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	(1b) 'business-to-business product with digital elements' means any product with digital elements' to be placed on the market with individual security configuration in accordance with contractual arrangements;

Or. en

Amendment 225
Evžen Tošenovský

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***	(2) 'remote data processing' means any ***remote*** data processing for which the software is designed and developed by ***or for*** the manufacturer, and ***is critical for the fundamental functions of*** the product with digital elements;

its functions;

Or. en

Amendment 226
Evžen Tošenovský

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

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

Or. en

Amendment 227
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
(4) 'highly critical product with digital elements' means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(5);	***deleted***

Or. en

Amendment 228
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 3 – paragraph 1 – point 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) 'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

Or. en

Justification

Reference to and alignment with the definition of cybersecurity found in the Cybersecurity Act.

Amendment 229
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 6

Text proposed by the Commission	*Amendment*
(6) 'software' means the part of an electronic information system which consists of computer code;	(6) 'software' means the part of an electronic information system which consists of computer code***, with exception of software relating to internet websites***;

Or. en

Amendment 230
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

Proposal for a regulation
Article 3 – paragraph 1 – point 11

Text proposed by the Commission	*Amendment*
(11) 'physical connection' means any connection between electronic information systems or components implemented using physical means, including through electrical or mechanical interfaces**,** wires ***or radio waves;***	(11) 'physical connection' means any connection between electronic information systems or components implemented using physical means, including through electrical or mechanical interfaces ***or*** wires**.**

Or. en

Amendment 231
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 16 a (new)

Text proposed by the Commission	*Amendment*
	(16a) 'micro, small and medium-sized enterprises' or 'SMEs' means micro, small and medium-sized enterprises as defined in the Annex to Commission Recommendation 2003/361/EC;

Or. en

Amendment 232
Ignazio Corrao
on behalf of the Verts/ALE Group

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 his or her name or trademark, whether for payment or ***monetisation***;

Or. en

Amendment 233
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation
Article 3 – paragraph 1 – point 21 a (new)

Text proposed by the Commission	*Amendment*

(21a) 'consumer' means any natural person who, under the circumstances of this Regulation, is acting for purposes which are outside their trade, business, craft or profession.

Or. en

Amendment 234
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 3 – paragraph 1 – point 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) 'micro, small and medium sized enterprises' means micro, small and medium sized enterprises as defined in Commission Recommendation 2003/361/EC[1a];
	[1a] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

Or. en

Amendment 235
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 3 – paragraph 1 – point 21 b (new)

Text proposed by the Commission	*Amendment*
	(21b) 'provider of an online marketplace' means a provider of an intermediary service using an online interface, which allows consumers to conclude distance contracts with traders for the sale of products;

Or. en

Justification

Adding a definition of an online marketplace, in line with Article 3 (1)(14) of the General Product Safety Regulation.

Amendment 236
Evžen Tošenovský

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***

Or. en

Amendment 237
Bart Groothuis

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 following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed***, excluding security and maintenances updates that aim to mitigate vulnerabilities***;

Or. en

Justification

Security updates should still be able to go through without delay by a conformity assessment.

Amendment 238
Evžen Tošenovský

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 ***by the manufacturer*** to the product with digital elements following its placing on the market, ***beyond necessary security and maintenance updates,*** which ***results in modification of the product's fundamental functions or its intended use and thus significantly*** affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I;

Or. en

Amendment 239
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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 ***or a series of changes*** 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;

Or. en

Amendment 240
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 34 a (new)

Text proposed by the Commission	*Amendment*
	(34a) 'international standard' means an international standard as defined in Article 2, point (1)(a), of Regulation (EU) No 1025/2012;

Or. en

Amendment 241
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 34 b (new)

Text proposed by the Commission	*Amendment*
	(34b) 'near miss' means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;

Or. en

Amendment 242
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 34 c (new)

Text proposed by the Commission	*Amendment*
	(34c) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

Or. en

Amendment 243
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 36 a (new)

Text proposed by the Commission	*Amendment*
	(36a) 'cyber threat' means a cyber threat as defined in Article 2, point (10), of Regulation (EU) 2019/881;

Or. en

Amendment 244
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 36 b (new)

Text proposed by the Commission	*Amendment*
	(36b) 'significant cyber threat' means a significant cyber threat as defined in Article 2, point (11), of Regulation (EU) 2019/881;

Or. en

Amendment 245
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 1 – point 37

Text proposed by the Commission	*Amendment*
(37) 'software bill of materials' means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;	(37) 'software bill of materials***' or 'SBOM***' means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;

Or. en

Amendment 246
Bart Groothuis

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 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; ***but does not include a vulnerability for which there is reliable evidence that the exploitation was performed by an actor for purposes of good faith testing, investigation, correction, or disclosure of a security flaw or vulnerability to promote the security or safety of the system owner, computers or software, or those who use such computers or software;***

Or. en

Justification

Vulnerability research should not be hindered.

Amendment 247
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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) '***known*** exploited vulnerability' means a ***patched*** vulnerability for which reliable evidence ***exists*** that execution of malicious code was performed by an actor on a system without permission of the system owner;

Or. en

Justification

Requiring the disclosure of a vulnerability should take place after that vulnerability has been patched or remedied, as the reporting of unpatched vulnerabilities could create significant new security risks that outweigh any potential benefits. This amendment is in line with ISO Standard ISO/IEC 29147, which requires disclosing a vulnerability only after the development and deployment of remediation.

Amendment 248
Bart Groothuis

Proposal for a regulation
Article 3 – paragraph 1 – point 39 – point a (new)

Text proposed by the Commission	*Amendment*
	a) 'expected product lifetime' means the lifetime a manufacturer documents in the information and instructions to the user defined in Annex II (8). For software it includes the iterated modifications within the version that was placed in the market.

Or. en

Justification

Corresponding definition used in Article 10.

Amendment 249
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 3 – paragraph 1 – point 39 a (new)

Text proposed by the Commission	*Amendment*
	(39a) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

Or. en

Justification

Reference to and alignment with the definition of incident found in the NIS-2 Directive.

Amendment 250
Ignazio Corrao
on behalf of the Verts/ALE Group

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 which does not comply with this Regulation.	2. Member States shall not prevent the presentation and use of a ***prototype*** product with digital elements ***or a software,*** which does not comply with this Regulation***, provided that the availability is limited in time and geographical area and is supplied exclusively for testing***.

Or. en

Amendment 251
Ignazio Corrao
on behalf of the Verts/ALE Group

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.	***deleted***

Or. en

Amendment 252
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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 software which does not comply with this Regulation.

Or. en

Amendment 253
Evžen Tošenovský

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 software which does not comply with this Regulation provided that the software is only made available ***in a non-production version*** for a limited period required for testing purposes***, including software labelled as "beta," "pre-release," or "candidate",*** 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.

Or. en

Amendment 254

Christophe Grudler, Valérie Hayer

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

Text proposed by the Commission	*Amendment*
	3a. This Regulation shall not prevent Member States from applying additional measures to products with digital elements provided that such measures are proportionate and aim to safeguard products, infrastructure or processed information and provided that those specific products are used for critical system functions or critical components deployed in sectors of high criticality as set out in Annex I to Directive (EU) 2022/2555.

Or. en

Justification

The maximal harmonisation nature of the regulation does not allow Member States to apply additional national requirements for regulated products, given that such additional requirements could prevent products that do not meet these additional requirements from accessing the market. It is important to preserve this ability of Member States to apply additional requirements for very specific use-cases and products with higher cybersecurity risks, in particular when national security is involved.

Amendment 255
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Or. en

Amendment 256
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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

Or. en

Amendment 257
Evžen Tošenovský

Proposal for a regulation
Article 6 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list of categories of critical products with digital elements a new category or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk	2. ***On the basis of the reports referred to in Article 56 and after consulting the Cyber Resilience Expert Group, ADCO, ENISA, and, where necessary, other relevant stakeholders,*** the Commission is empowered to adopt delegated acts***,*** in accordance with Article 50 to amend Annex III by including in the list of categories of critical products with digital

related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into account:

elements a new category or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into account:

Or. en

Amendment 258
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

Proposal for a regulation
Article 6 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list of categories of critical products with digital elements a new category or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into account:	2. The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list of categories of critical products with digital elements a new category or withdrawing an existing one from that list***.*** ***The Commission should carry out periodical checks to assess whether the list of critical products with digital elements needs to be integrated or updated***. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into account:

Or. en

Amendment 259
Evžen Tošenovský

Proposal for a regulation

Article 6 – paragraph 3

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

Or. en

Amendment 260
Bart Groothuis

Proposal for a regulation
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by 12 months since the entry into force of this Regulation].	3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. ***If it expands the scope of the product categories, the procedure in paragraph 2 should be followed.*** The delegated act shall be adopted [by 12 months since the entry into force of this Regulation]. ***The Commission shall establish a process under which a product which is a candidate to be a critical product can be reviewed in a collaborative process by all relevant stakeholders, including manufacturers and users, to assess the security risk posed by potential cybersecurity issues with the product, whether and how much designating the product as critical would likely reduce that risk, and the costs associated with designating the product as critical. If such assessment clearly establishes that designating that product as critical would materially reduce the security risk posed***

	to the users of the product and that the value of such reduction would outweigh the costs to the manufacturer and other parties, the product may be designated as critical under this Regulation.

Or. en

Justification

This indicates that the initial scope of the CRA is not clearly stated from the beginning, and may be subject to changes. This should not be the case. If not deleted, guardrails should be introduced.

Amendment 261
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by ***12*** months since the entry into force of this Regulation].	3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by ***9*** months since the entry into force of this Regulation].

Or. en

Amendment 262
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product	3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product

categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by ***12*** months since the entry into force of this Regulation].	categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by ***6*** months since the entry into force of this Regulation].

Or. en

Amendment 263
Ignazio Corrao
on behalf of the Verts/ALE Group

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).***

Or. en

Amendment 264
Bart Groothuis

Proposal for a regulation
Article 6 – 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 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	***deleted***

categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:

(a) used or relied upon by the essential entities of the type referred to in Annex [Annex I] to the Directive [Directive XXX/ XXXX (NIS2)] or will have potential future significance for the activities of these entities; or

(b) relevant for the resilience of the overall supply chain of products with digital elements against disruptive events.

Or. en

Justification

The Commission is already empowered to amend the lists of critical products. If a product is in the future considered 'highly critical,' it should simply be included anew under Class II of Annex III to ensure a heightened level of conformity assessment. Requiring mandatory certification here overlaps with considerations regarding the use of critical products by essential entities covered by NIS2, but could also risk sidestepping the traditional approach to standardization that is based on coordinated efforts by the technical and industry community.

Amendment 265
Evžen Tošenovský

Proposal for a regulation
Article 6 – 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 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	***deleted***

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

(a) used or relied upon by the essential entities of the type referred to in Annex [Annex I] to the Directive [Directive XXX/ XXXX (NIS2)] or will have potential future significance for the activities of these entities; or

(b) relevant for the resilience of the overall supply chain of products with digital elements against disruptive events.

Or. en

Amendment 266
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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 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	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 certification scheme ***at assurance level "high"*** pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with

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:	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:

Or. en

Amendment 267
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation
Article 9 – paragraph 1 – subparagraph 1 (new)

Text proposed by the Commission	*Amendment*
	Internal networks of a machinery product with digital elements are not subject to this Regulation when they are secured via dedicated endpoints and isolated from external networks, and where the manufacturer assess and indicate the intended final use of the component for the sole internal operations and communication.

Or. en

Amendment 268
Zdzisław Krasnodębski, Adam Bielan, Kosma Złotowski

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 12 months from placing a software on the market.

Or. en

Amendment 269
Bart Groothuis

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 produced in accordance with the essential requirements set out in Section 1 of Annex I. ***Manufacturers may deviate from a requirement in justified cases if it does not apply due to the nature of the product. Manufacturers should document the justification in the cybersecurity risks assessment in accordance to paragraph 2.***

Or. en

Justification

Not all of requirements are relevant to each and every manufacture's product. This should be clarified and justified.

Amendment 270
Evžen Tošenovský

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 ***take reasonable measures*** that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.

Or. en

Amendment 271
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

Proposal for a regulation
Article 10 – paragraph 2

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

Or. en

Amendment 272
Ignazio Corrao
on behalf of the Verts/ALE Group

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	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

security of the product with digital elements.	compromise the security of the product with digital elements***, in particular in the case of open source software that have not been placed on the market in exchange of financial or other type of monetisation, including data returns***. ***The due diligence obligation can be considered fulfilled if all components have been already deemed compliant and the CE mark has been affixed to them as appropriate.***

Or. en

Amendment 273
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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***, including when they integrate components of open-source software that have not been supplied in the course of a commercial activity***. They shall ensure that such components do not compromise the security of the product with digital elements.

Or. en

Amendment 274
Evžen Tošenovský

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,	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.	manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ***take reasonable measures*** ensure that such components do not compromise the security of the product with digital elements.

Or. en

Amendment 275
Ignazio Corrao
on behalf of the Verts/ALE Group

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, for ***a period of at least five years or*** the expected product lifetime or, 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. ***In the case of small and micro enterprises this obligation and the obligation foreseen in Article 10(12) are limited to the expected product lifetime as determined by the manufacturer, taking into account the reasonable expectations of consumers regarding the functionality, intended purpose of the product, and the provision of security and functionality updates. In any case, the end users must be informed of the minimal duration that a product will benefit from security updates, before purchase. Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources. Those procedures shall***

differentiate between security updates that provide devices with enhanced security, including security patches and corrective or functionality updates that provide corrective or new functionalities, including corrective patches, establishing that these updates should be provided separately, unless clearly demonstrated that it is not technically possible. The end user shall always retain the possibility to revert to a previous version of functionality updates.

Or. en

Amendment 276
Evžen Tošenovský

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 ***indicated by the manufacturer,*** 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. ***The Commission may, after consulting the Cyber Resilience Expert Group, ADCO, ENISA, and, where necessary, other relevant stakeholders, by means of implementing acts, specify the format and information of the label for consumer products with digital elements, which might easily indicate the expected lifetime of the product. On top of that, this label might contain additional information enabling consumers to quickly understand the level of security and privacy associated with the product. Those***

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

Or. en

Amendment 277
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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, ***the manufacturer shall define*** the expected product lifetime***. In doing so, the manufacturer shall ensure that expected*** product ***lifetime is in line with reasonable consumer expectations and that it promotes sustainability and the need to ensure long-lasting products with digital elements.*** 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 ***during at least the expected product lifetime or 10 years, whichever is shorter***. ***Where applicable, the expected product lifetime shall be clearly stated on the product, its packaging or be included in contractual agreements.***

Or. en

Amendment 278
Bart Groothuis

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

Text proposed by the Commission	*Amendment*
When placing a product with digital	***Manufacturers shall ensure,*** when placing

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.	a product with digital elements on the market and for the expected product lifetime, that vulnerabilities of that product ***or of its iterated versions during its lifetime*** are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I. ***Manufacturers shall determine the expected product lifetime referred to in the first subparagraph of this paragraph taking into account the time users reasonably expect to be able to use the product given its functionality and intended purpose and therefore can expect to receive security updates***

Or. en

Justification

By setting as a main rule that the support period should cover the expected product lifetime, in combination with the transparency about the duration of this expected product lifetime (and therefore support period) proposed below, manufacturers are encouraged to choose a reasonable support period that can be longer than 5 years.

Amendment 279
Christophe Grudler, Valérie Hayer

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.	***Manufacturers shall ensure,*** when placing a product with digital elements on the market and for the expected product lifetime, that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I. ***The expected product lifetime shall not be less than five years for products covered by Directive 2009/125/EC of the European Parliament and of the Council[1a].***

[1a] Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products (OJ L 285, 31.10.2009, p. 10).

Or. en

Justification

Many products should be relied on for much longer than five years. The five-year maximum could lead economic operators to only provide cybersecurity support for five years. Establishing a defined minimum or maximum period of time does not seem effective. A proposal is made to make a link with the ecodesign directive, highlighting the importance of durability of products, including the handling of vulnerabilities.

Amendment 280
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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

Or. en

Justification

The support period should cover the expected product lifetime. The support period should be based on a time period that users can reasonably expect to be able to use the product, given its functionality and purpose.

Amendment 281
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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, 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. ***Where applicable, the expected product lifetime shall be stated on the product or be included in contractual agreements.***

Or. en

Amendment 282
Christophe Grudler, Valérie Hayer

Proposal for a regulation
Article 10 – paragraph 6 – subparagraph 1 a (new)

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

Or. en

Justification

The support period should be based on the time users reasonably expect to be able to use the product given its functionality and intended purpose. In order to avoid a race to the bottom which would undermine its effectiveness, Article 10 (6) should also prescribe how the manufacturer is to determine the expected product lifetime referred to in the first subparagraph.

Amendment 283
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 10 – paragraph 6 – subparagraph 2 a (new)

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

Or. en

Justification

The support period should cover the expected product lifetime. The support period should be based on a time period that users can reasonably expect to be able to use the product, given its functionality and purpose.

Amendment 284
Evžen Tošenovský

Proposal for a regulation
Article 10 – paragraph 7 – subparagraph 1

Text proposed by the Commission	*Amendment*
Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23.	Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23. ***The technical documentation shall be made available by the manufacturers, to the market surveillance authorities or CSIRTs, upon justified request, for the purpose of specific supervisory tasks and incident handling set in this Regulation. Those authorities shall ensure the confidentiality and appropriate protection of the information provided in the technical documentation.***

Or. en

Amendment 285
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

Proposal for a regulation
Article 10 – paragraph 8

Text proposed by the Commission	*Amendment*
8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.	8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years***, or for the expected product lifetime, whichever is longer,*** after the product with digital elements has been placed on the market.

Or. en

Amendment 286
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 10 – paragraph 8

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

Or. en

Amendment 287
Marc Botenga

Proposal for a regulation

Article 10 – paragraph 8

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

Or. en

Amendment 288
Evžen Tošenovský

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 ***or international*** 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 for future product generations. The manufacturer shall take into account the associated costs and efforts, including the efforts required for development, testing, validation and approval process time.***

Or. en

Amendment 289
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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 ***horizontal or domain specific*** standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.

Or. en

Amendment 290
Bart Groothuis

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	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.	elements and changes in the harmonised ***or industry*** standards, European cybersecurity certification schemes by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.

Or. en

Justification

To reflect the deletion in article 19.

Amendment 291
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	9a. Manufacturers shall publicly communicate and advertise the expected product lifetime of their products, in a clear and understandable manner, and in particular, the minimal duration of the provision of security updates.

Or. en

Amendment 292
Marc Botenga

Proposal for a regulation
Article 10 – paragraph 10

Text proposed by the Commission	*Amendment*
10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such	10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such

information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements.	information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements. ***The expected product lifetime shall be communicated and advertised in a clear manner by the manufacturers, and where feasible the expected lifetime shall be clearly demonstrated on the packaging of the product.***

Or. en

Amendment 293
Bart Groothuis

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

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

Or. en

Justification

By setting as a main rule that the support period should cover the expected product lifetime, in combination with the transparency about the duration of this expected product lifetime (and therefore support period) proposed below, manufacturers are encouraged to choose a reasonable support period that can be longer than 5 years.

Amendment 294
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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

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

Or. en

Justification

Users should be clearly informed about the expected product lifetime during which the manufacturer will provide security updates or otherwise effectively handle vulnerabilities.

Amendment 295
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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	12. From the placing on the market and for the expected product lifetime, 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

product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.	appropriate.

Or. en

Amendment 296
Evžen Tošenovský

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 ***indicated by the manufacturer in accordance with paragraph 6 of this Article,*** 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.

Or. en

Amendment 297
Marc Botenga

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***	12. From the placing on the market and for the ***entire*** expected ***lifespan*** of a product with digital elements,

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.

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.

Or. en

Amendment 298
Ignazio Corrao
on behalf of the Verts/ALE Group

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 ***for a period of at least five years or*** for the expected product lifetime, 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.

Or. en

Amendment 299
Evžen Tošenovský

Proposal for a regulation
Article 10 – paragraph 13 a (new)

Text proposed by the Commission	*Amendment*
	13a. For the purposes of complying with the obligations laid down in this Regulation, manufacturers shall ensure that they use adequate skilled professionals in the field of cybersecurity.

Or. en

Amendment 300
Bart Groothuis

Proposal for a regulation
Article 10 – paragraph 15

Text proposed by the Commission	*Amendment*
15. The Commission may, by means of implementing acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	15. The Commission may, by means of implementing acts***, and following an open consultation with stakeholders and in line with international standards***, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Or. en

Justification

Industry consultations, best practices, or standards ought to be taken into consideration.

Amendment 301
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 10 – paragraph 15

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

Or. en

Amendment 302
Evžen Tošenovský

Proposal for a regulation
Article 10 – paragraph 15

Text proposed by the Commission	*Amendment*
15. The Commission may, by means of ***implementing acts***, specify the format and elements of the ***software bill of materials*** set out in Section 2, point (1), of Annex I***.*** ***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2)***.	15. The Commission may, ***after consulting the Cyber Resilience Expert Group, ADCO, ENISA, and, where necessary, other relevant stakeholders,*** by means of ***guidelines***, specify the ***recommended*** format and elements of the ***SBOMs*** set out in Section 2, point (1), of Annex I***, based on international standards and established best practices***.

Or. en

Amendment 303
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

Proposal for a regulation
Article 10 – paragraph 15

Text proposed by the Commission	*Amendment*
15. The Commission may, by means of ***implementing*** acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those ***implementing*** acts shall be adopted in accordance with ***the examination***	15. The Commission may, by means of ***delegated*** acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those ***delegated*** acts shall be adopted in accordance with Article ***50***.

procedure referred to in Article ***51(2)***.

Or. en

Amendment 304
Evžen Tošenovský

Proposal for a regulation
Article 10 a (new)

Text proposed by the Commission	*Amendment*
	Article10a
	Reporting of vulnerabilities
	1. The manufacturer shall, without undue delay, notify to CSIRT in the Member State of main establishment designated as a coordinator for the purposes of coordinated vulnerability disclosure in accordance with Article 12(1) of Directive 2022/2555 of Member States concerned any patched vulnerability contained in the product with digital elements and may voluntarily notify, where appropriate, also the unpatched vulnerability. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken, in particular regarding available patches. The mere act of notification of vulnerability shall not subject the notifying manufacturer to increased liability. CSIRT designated as a coordinator shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the upon receipt to ENISA and inform the market surveillance authorities concerned about the notified vulnerability.
	2. The information about vulnerability shall be stored in a European vulnerability database referred to in Article 12(2) of Directive 2022/2555, maintained by ENISA. That database shall include: (a) information describing the vulnerability; (b) the affected product

with digital elements and the severity of the vulnerability in terms of the circumstances under which it may be exploited; (c) the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable product with digital elements as to how the risks resulting from disclosed vulnerabilities can be mitigated.

3. Natural or legal persons shall be able to report, anonymously where they so request, a vulnerability of product with digital elements to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall without undue delay notify the manufacturer, ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where the reporting concerns the manufacturer with main establishment in other Member State, the CSIRT designated as coordinator shall forward it to relevant CSIRT designated as coordinator in that Member State. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

Or. en

Amendment 305
Evžen Tošenovský

Proposal for a regulation
Article 11 – title

Text proposed by the Commission	*Amendment*

Or. en

Amendment 306
Evžen Tošenovský

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.	***deleted***

Or. en

Amendment 307
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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	1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any ***known*** 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.

contained in the product with digital elements ***in accordance with paragraph 1a of this Article***. 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 ***(EU) 2022/2555 (NIS2)*** of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability. ***Where a notified vulnerability has no corrective or mitigating measures available, ENISA shall ensure that the sharing of information regarding the notified vulnerability is based on applicable security protocols and on a need-to-know-basis.***

Or. en

Justification

The timetable for reporting and information to be included are aligned with NIS 2 (paragraph 1a). In order to mitigate the possibility of further cybersecurity risks, information about unpatched vulnerabilities shall not be distributed.

Amendment 308
Ignazio Corrao
on behalf of the Verts/ALE Group

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,	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.

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 inform the market surveillance authority about the ***existence of a*** vulnerability ***and where applicable, the potential risk mitigation measures*** .

Or. en

Amendment 309
Bart Groothuis

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 ***72*** hours ***after the patch is publicly available***, notify to ***CSIRT Network any new patched vulnerabilities*** contained in the product with digital elements ***that may be actively exploited and pose a significant cybersecurity risk***. The notification shall include ***basic*** details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken ***based on the manufacturers*** coordinated vulnerability disclosure ***policy required by section 2 of Annex I item (5) (e.g., the ISO/IEC 29147)***.

Or. en

Justification

Mandatory reporting of unpatched exploited vulnerabilities to ENISA is dangerous as these vulnerabilities can be exploited, and against coordinated vulnerability disclosure processes. In no case should there be a central database of unpatched vulnerabilities. It would effectively make ENISA world's largest honey pot. If not deleted, it could be revised to only require reporting of patched vulnerabilities (to avoid exploitation) within 72 hours after the patch publicly is available, following industry best practices and standards as a baseline for wider EU coordinated vulnerability disclosure.

Amendment 310
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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

Text proposed by the Commission	*Amendment*
	1a. 1a. Notifications as referred to in paragraph 1 shall be subject to the following procedure:
	(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the known exploited vulnerability, detailing whether any known corrective or mitigating measure is available;
	(b) a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the known exploited vulnerability, which, where applicable, updates the information referred to in point (a), details any corrective or mitigating measures taken and indicates an assessment of extent of the vulnerability, including its severity and impact;
	(c) an intermediate report on relevant status updates, upon the request of ENISA;
	(d) a final report, within one month after the submission of the vulnerability notification under point (b), including at least the following:
	(i) a detailed description of the

vulnerability, including its severity and impact;

(ii) where available, information concerning any actor that has exploited or that is exploiting the vulnerability;

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

Or. en

Justification

Alignment with NIS-2 Directive.

Amendment 311
Angelika Niebler

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

Text proposed by the Commission	*Amendment*
	1a. Manufacturers shall submit to ENISA a vulnerability notification within 72 hours of becoming aware of the actively exploited vulnerability, which, where applicable, shall update the information that was given in the early warning, especially on the corrective or mitigating measures taken.

Or. en

Amendment 312
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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

Text proposed by the Commission	*Amendment*
	1b. Once a security update has been made available, or an appropriate corrective or mitigation measure has been

implemented, ENISA shall add the notified vulnerability to the European vulnerability database referred to in Article 12 of Directive [Directive 2022/2555 (NIS2)].

Or. en

Amendment 313
Evžen Tošenovský

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 ***notify***, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA ***its CSIRT in the Member State of main establishment of*** any incident ***that has a significant*** impact on the security of the product with digital elements ***as referred to in paragraph 2a (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 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. ***The mere act of notification shall not subject the notifying manufacturer to increased liability.*** ***On a voluntary basis, the manufacturer may notify also other than significant incidents, cyber threats and near misses.***

Or. en

Amendment 314
Bart Groothuis

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, notify ***the designated CSIRT or single point of contact, in accordance to the procedure of Directive [Directive XXX.XXXX NIS2], any significant*** incident having impact on the security of the product with digital elements. ***The single point of contact*** shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned 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.

Or. en

Justification

This is to align with the reporting procedure under the NIS2 to avoid conflicting reporting requirements. Alternatively, it could inform the CSIRT network directly.

Amendment 315
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Angelika Niebler, Adam Jarubas

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 notify to ENISA any ***significant*** incident having impact on the security of the product with digital elements ***in accordance with paragraph 2b of this Article***. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive ***(EU) 2022/2555 (NIS2)*** of the Member States concerned and inform the market surveillance authority about the notified ***significant*** incidents. The ***significant*** incident notification shall include ***the necessary*** information ***to make the competent authority aware*** of the incident and ***allow for the entity to seek assistance***.

Or. en

Justification

Following the approach in NIS 2, only significant incidents should be reported on a mandatory basis. In this regard, the timetable for notifications should also be aligned in paragraph 2b.

Amendment 316
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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

Text proposed by the Commission	*Amendment*
	2a. An incident shall be considered to be significant, where:
	(a) it has caused or is capable of causing severe operational disruption of the production or the services for the manufacturer concerned, which would impact the security of a product; or

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

Or. en

Justification

Aligning the Article with NIS2 definition of significant incident. Only significant incidents affecting the security of the product should be reported on a mandatory basis, to avoid overburdening manufacturers or ENISA.

Amendment 317
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	2a. An incident shall be considered to be significant if:
	(a) it has caused or is capable of causing severe operational disruption of the design, development, production or functioning of the product with digital elements or financial loss for the manufacturer concerned;
	(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Or. en

Amendment 318
Bart Groothuis

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

Text proposed by the Commission	*Amendment*
	2a. Economic operators that are also identified as essential entities or important

entities under the Directive [Directive XXX.XXXX NIS2] and who submit their incident notification pursuant to the Directive [Directive XXX.XXXX NIS2] should be deemed compliant with the requirements in point 2 of this Article. Moreover, an entity may only be fined once for non-compliance to overlapping reporting requirements.

Or. en

Justification

To streamline reporting obligations with the NIS2, avoid overlap and double fines.

Amendment 319
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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

Text proposed by the Commission	*Amendment*
	2b. Notifications as referred to in paragraph 2 shall be subject to the following procedure:
	(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the significant incident, which, where applicable, indicates whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
	(b) an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the significant incident, which, where applicable, updates the information referred to in point (a) and indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
	(c) an intermediate report on relevant status updates upon the request of

ENISA;

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

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

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

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident; In the event of an ongoing incident at the time of the submission of the final report referred to in point (d) of the first subparagraph, Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

Or. en

Justification

Alignment with NIS2 Directive.

Amendment 320
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	2b. For the purpose of notification under paragraph 1, the manufacturers concerned submit to the CSIRT:
	(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-

border impact;

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

(c) upon the request of a CSIRT an intermediate report on relevant status updates; (d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

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

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

(iii) applied and ongoing mitigation measures;

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

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

Or. en

Amendment 321
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	2c. CSIRT shall, without undue delay, unless for justified cybersecurity risk-

related grounds, inform the market surveillance authority about the notified incidents and in the case of a cross-border significant incident forward the notifications to the single point of contact designated in accordance with Article 8(3) of Directive (EU) 2022/2555.

Or. en

Amendment 322
Evžen Tošenovský

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

Or. en

Amendment 323
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 11 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. ENISA shall publish and maintain a known exploited vulnerability catalogue that shall be included in the European vulnerability database established under Directive 2022/2555 (NIS2). The catalogue shall assist manufacturers in detecting known exploitable

vulnerabilities and notify vulnerabilities found in their products.

Or. en

Amendment 324
Evžen Tošenovský

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. ***Where appropriate,*** the manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the ***significant*** incident ***having major impact on the security of the product concerned,*** and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the ***significant*** incident.

Or. en

Amendment 325
Bart Groothuis

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 ***impacted*** users of the product with digital elements about the incident ***having significant impact*** and, where necessary ***may inform all users of the product with digital elements***, about corrective measures that the user can deploy to mitigate the impact of the incident.

Or. en

Justification

To align with NIS2 (significant impact) and not to lose the benefit of a notification but keep those obligations manageable and relevant.

Amendment 326
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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 and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the ***significant*** incident.

Or. en

Justification

Alignment with NIS2 Directive, following the approach of the preceding amended paragraphs of this Article.

Amendment 327
Ignazio Corrao
on behalf of the Verts/ALE Group

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 incident and, where necessary, about ***risk mitigation and any*** corrective measures that the user can deploy to mitigate the impact of the incident.

Or. en

Amendment 328
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	4a. The CSIRT shall provide, without undue delay and where possible within 24 of receiving the early warning referred to in paragraph 4, point (a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity may provide guidance or operational advice on the implementation of possible mitigation measures. The CSIRT may provide additional technical support if the manufacturer concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT shall provide guidance on reporting the significant incident to law enforcement authorities. CSIRTs may prioritise the processing of mandatory notifications over voluntary notifications, as well as processing of notifications related to critical products with digital elements over other products with digital elements.

Or. en

Amendment 329
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	4b. As appropriate, the CSIRT shall inform market surveillance authority

concerned and forward to it, on request, relevant information, on the incident handling, particularly as regards the final report referred to in paragraph 2b(e) of this Article.

Or. en

Amendment 330
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	4c. Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 2b. In so doing, the CSIRT or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

Or. en

Amendment 331
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	4d. Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant

incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so

Or. en

Amendment 332
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	4e. At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.

Or. en

Amendment 333
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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 the examination procedure referred to in Article 51(2)***.	5. The Commission ***is empowered to adopt delegated*** acts, ***in accordance with Article 50, to*** further ***specify*** the type of information, format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those ***delegated*** acts shall be adopted ***within 9 months of entry into force of this Regulation***.

Or. en

Amendment 334
Evžen Tošenovský

Proposal for a regulation
Article 11 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. The Commission may adopt, after consulting stakeholders and CSIRTs Network, by means of implementing acts, further specifying further the type of information, format and the procedure of the a notifications and submitted pursuant to paragraphs 1 and 2 of this Article and of a information submitted pursuant to paragraph 4 of this Article and common notification templates for the single reporting under relevant EU law in accordance with Article 11a. Those implementing acts shall be based, where relevant, on European and international standards and shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Or. en

Amendment 335
Ignazio Corrao
on behalf of the Verts/ALE Group

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. ***Such corrective or mitigating measures shall be accompanied by the relevant code and appropriate licenses that allow the deployment. 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.***

Or. en

Amendment 336
Marc Botenga

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 to the person or entity maintaining the component. ***Software modifications in a component developed by manufacturers in order to address reported vulnerabilities shall be shared, including the relevant code, to the person or entity maintaining the component.***

Or. en

Amendment 337
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Angelika Niebler

Proposal for a regulation
Article 11 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*

7a. ENISA shall establish a digital reporting mechanism, after having consulted relevant stakeholder groups, so that manufacturers are able to fulfil their reporting obligations via an Online Application.

Or. en

Amendment 338
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 11 a (new)

Text proposed by the Commission	*Amendment*
	Article11a
	Single point of contact for users
	1. Manufacturers shall designate a single point of contact to enable users to communicate directly and rapidly with them, where applicable by electronic means and in a user-friendly manner, including by allowing recipients of the service to choose the means of communication, which shall not solely rely on automated tools.
	2. In addition to the obligations provided under Directive 2000/31/EC, manufacturers shall make public the information necessary for the end users in order to easily identify and communicate with their single points of contact. That information shall be easily accessible and shall be kept up to date.

Or. en

Amendment 339
Evžen Tošenovský

Proposal for a regulation
Article 11 a (new)

Text proposed by the Commission	*Amendment*
	Article11a
	Single Entry Point
	For the purpose of simplifying reporting and of implementing the automatic and direct reporting and forwarding mechanism under Articles 10a and 11 this Regulation, Directive (EU) 2022/2555, and possibly under other relevant EU legislation, such as Regulation (EU) 2016/679, Member States shall establish and use a single entry point.

Or. en

Amendment 340
Evžen Tošenovský

Proposal for a regulation
Article 12 – paragraph 1

Text proposed by the Commission	*Amendment*
1. A manufacturer may appoint an authorised representative by a written mandate.	1. A manufacturer may appoint an authorised representative***(s) for all Member States markets or for specific Member States*** by a written mandate.

Or. en

Amendment 341
Bart Groothuis

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

Text proposed by the Commission	*Amendment*
	(ca) Non-technical risk factors of the manufacturer are taken into consideration for critical products described in Class II of Annex III intended for the use by essential entities of the type referred to in [Annex I to the

Directive XXX/XXXX (NIS2)];

Or. en

Justification

The CRA has a missed opportunity to not address the issue of risky vendors, especially in the context of critical infrastructure. While there have been positive developments towards non-binding toolboxes to address specific supply chain security issues related 5G (toolbox) the European Court of Auditors concluded that since the 5G toolbox was adopted, progress has been made to reinforce the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors, but that none of the measures put forward are legally binding, meaning that implementation across the Union is inconsistent at best, and that the Commission has no power to enforce those rules. This should be addressed in the Cyber Resilience Act.

Amendment 342
Ignazio Corrao
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 343
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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	3. Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in

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

Or. en

Justification

The Commission proposal presupposes that importers should have in-depth knowledge of the significance of cybersecurity risks, which is challenging for small and medium-scale enterprises in particular. Instead, distributors should inform of any cybersecurity risk and it is for the manufacturer with more available resources to react and assess the severity of the risk.

Amendment 344
Ignazio Corrao
on behalf of the Verts/ALE Group

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 set out in Annex I, or to withdraw or recall the product, if appropriate.	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. ***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.***

Or. en

Amendment 345
Bart Groothuis

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 set out in Annex I, or to withdraw or recall the product, if appropriate.	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 ***or non-technical risk factors*** 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.

Or. en

Justification

The CRA has a missed opportunity to not address the issue of risky vendors, especially in the context of critical infrastructure. While there have been positive developments towards non-binding toolboxes to address specific supply chain security issues related 5G (toolbox) the European Court of Auditors concluded that since the 5G toolbox was adopted, progress has been made to reinforce the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors, but that none of the measures put forward are legally binding, meaning that implementation across the Union is inconsistent at best, and that the Commission has no power to enforce those rules. This should be addressed in the Cyber Resilience Act.

Amendment 346
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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 set out in Annex I, or to withdraw or recall the product, if appropriate.	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 ***require the manufacturer to*** take the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity with the essential requirements set out in Annex I, or to withdraw or recall the product, if appropriate.

Or. en

Justification

As importers are often small and medium-sized enterprises, compared to larger manufacturers, it may be overly burdensome for importers to ensure that corrective measures are taken. Manufacturers, that often are larger enterprises, are better equipped to take care of corrective measures.

Amendment 347
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 13 – paragraph 6 – subparagraph 2

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

Or. en

Justification

As importers are often small and medium-sized enterprises, compared to larger manufacturers, it may be overly burdensome for importers to ensure that corrective measures are taken. Manufacturers, that often are larger enterprises, are better equipped to take care of corrective measures.

Amendment 348
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 13 – paragraph 6 – subparagraph 2 a (new)

Text proposed by the Commission	*Amendment*
	Upon receiving information from the manufacturer that the product with digital elements presents a significant cybersecurity risk, giving details, in particular, of the non-conformity and of any corrective measures taken, importers shall immediately forward this information to the market surveillance authorities of the Member States in which they made the product with digital elements available on the market to that effect.

Or. en

Justification

As importers are often small and medium-sized enterprises, compared to larger manufacturers, it may be overly burdensome for importers to ensure that corrective measures are taken. Manufacturers, that often are larger enterprises, are better equipped to take care of corrective measures.

Amendment 349
Bart Groothuis

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

Text proposed by the Commission	*Amendment*
	(ba) Non-technical risk factors of the manufacturer are taken into

consideration for critical products described in Class II of Annex III intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];

Or. en

Justification

The CRA has a missed opportunity to not address the issue of risky vendors, especially in the context of critical infrastructure. While there have been positive developments towards non-binding toolboxes to address specific supply chain security issues related 5G (toolbox) the European Court of Auditors concluded that since the 5G toolbox was adopted, progress has been made to reinforce the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors, but that none of the measures put forward are legally binding, meaning that implementation across the Union is inconsistent at best, and that the Commission has no power to enforce those rules. This should be addressed in the Cyber Resilience Act.

Amendment 350
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	(ba) they have received from the importer all the information and documentation required by this regulation.

Or. en

Amendment 351
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 14 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where a distributor considers or has reason to believe that a product with digital	3. Where a distributor considers or has reason to believe that a product with digital

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

Or. en

Justification

The Commission proposal presupposes that distributors should have in-depth knowledge of the significance of cybersecurity risks, which is challenging for small and medium-scale enterprises in particular. Instead, distributors should inform of any cybersecurity risk and it is for the manufacturer with more available resources to react and assess the severity of the risk.

Amendment 352
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 14 – paragraph 4 – subparagraph 1

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

Or. en

Justification

As distributors are often small and medium-sized enterprises compared larger to manufacturers, it may be overly burdensome for importers to ensure that corrective measures are taken. Manufacturers, that often are larger enterprises, are better equipped to take care of corrective measures.

Amendment 353
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 14 – paragraph 4 – subparagraph 2

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

Or. en

Justification

As distributors are often small and medium-sized enterprises compared larger to manufacturers, it may be overly burdensome for importers to ensure that corrective measures are taken. Manufacturers, that often are larger enterprises, are better equipped to take care of corrective measures.

Amendment 354
Bart Groothuis

Proposal for a regulation
Article 14 – paragraph 4 – subparagraph 2

Text proposed by the Commission	*Amendment*

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

Or. en

Justification

The CRA has a missed opportunity to not address the issue of risky vendors, especially in the context of critical infrastructure. While there have been positive developments towards non-binding toolboxes to address specific supply chain security issues related 5G (toolbox) the European Court of Auditors concluded that since the 5G toolbox was adopted, progress has been made to reinforce the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors, but that none of the measures put forward are legally binding, meaning that implementation across the Union is inconsistent at best, and that the Commission has no power to enforce those rules. This should be addressed in the Cyber Resilience Act.

Amendment 355
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 14 – paragraph 4 – subparagraph 2 a (new)

Text proposed by the Commission	*Amendment*
	Upon receiving information from the manufacturer that the product with digital elements presents a significant cybersecurity risk, giving details, in particular, of the non-conformity and of any corrective measures taken, distributors shall immediately forward this information to the market surveillance authorities of the Member States in which they made the product

with digital elements available on the market to that effect.

Or. en

Justification

As distributors are often small and medium-sized enterprises compared larger to manufacturers, it may be overly burdensome for importers to ensure that corrective measures are taken. Manufacturers, that often are larger enterprises, are better equipped to take care of corrective measures.

Amendment 356
Ignazio Corrao
on behalf of the Verts/ALE Group

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 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.

Or. en

Amendment 357
Marc Botenga

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	A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements ***and commercially supplies it in the market,*** shall be considered a

Regulation.	manufacturer for the purposes of this Regulation.

Or. en

Amendment 358
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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 carries out a substantial modification of the product with digital elements***, with the intention of making a profit,*** shall be considered a manufacturer for the purposes of this Regulation.

Or. en

Amendment 359
Nicola Danti

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 carries out a substantial modification of the product with digital elements ***and makes it available on the market*** shall be considered a manufacturer for the purposes of this Regulation.

Or. en

Justification

Clarification to explicitly state that this article only applies when a product is substantially modified and then made available on the market, e.g. contributions from individuals to open

source projects should not lead to them being considered as manufacturers.

Amendment 360
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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 carries out a substantial modification of the product with digital elements***, making it available on the market,*** shall be considered a manufacturer for the purposes of this Regulation.

Or. en

Amendment 361
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 17 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. Economic operators shall, on request ***and where the information is available***, provide to the market surveillance authorities the following information:	1. Economic operators shall, on request, provide to the market surveillance authorities the following information:

Or. en

Amendment 362
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 17 a (new)

Text proposed by the Commission	*Amendment*

Article17a

Specific obligations of providers of online marketplaces

1. Without prejudice to the general obligations provided for in Article 11 of Regulation (EU) 2022/2065, providers of online marketplaces shall designate a single point of contact allowing for direct communication, by electronic means, with Member States' market surveillance authorities in relation to cybersecurity issues.

2. Without prejudice to the general obligations provided for in Article 12 of Regulation (EU) 2022/2065, providers of online marketplaces shall designate a single point of contact to enable consumers to communicate directly and rapidly with them in relation to cybersecurity issues.

3. As regards powers conferred by Member States in accordance with Article 14 of Regulation (EU) 2019/1020, Member States shall confer on their market surveillance authorities the necessary power, as regards specific content referring to an offer of a product with digital elements, which presents a significant cybersecurity risk or a vulnerability, to issue an order requiring the providers of online marketplaces to remove such content from their online interface, to disable access to it or to display an explicit warning. Such orders shall be issued in accordance with the minimum conditions set out in Article 9(2) of Regulation (EU) 2022/2065. Providers of online marketplaces shall take the necessary measures to receive and process orders issued pursuant to this paragraph and they shall act without undue delay.

4. Orders issued pursuant to paragraph 4 may require the provider of an online marketplace, for the prescribed period, to remove from its online interface all identical content referring to an offer of the product in question, to disable access

to it or to display an explicit warning, provided that the search for the content concerned is limited to the information identified in the order and does not require the provider of an online marketplace to carry out an independent assessment of that content, and that the search and the removal can be carried out in a proportionate manner by reliable automated tools.

5. Providers of online marketplaces shall, without undue delay, process the notices related to cybersecurity issues with regard to the product offered for sale online through their services, received in accordance with Article 16 of Regulation (EU) 2022/2065.

6. For the purpose of compliance with the requirements of Article 31(1) and (2) of Regulation (EU) 2022/2065 as regards product safety information, providers of online marketplaces shall design and organise their online interface in a way that enables traders offering the product to provide at least the following information for each product offered and that ensures that the information is displayed or otherwise made easily accessible by consumers on the product listing: (a) name, registered trade name or registered trade mark of the manufacturer, as well as the postal and electronic address at which the manufacturer can be contacted; (b) information allowing the identification of the product, including a picture of it, its type and any other product identifier; and (c) any warning or safety information to be affixed on the product or to accompany it in accordance with this Regulation or the applicable Union harmonisation legislation in a language which can be easily understood by consumers as determined by the Member State in which the product is made available on the market.

7. For the purpose of compliance with Article 23 of Regulation (EU) 2022/2065

regarding cybersecurity issues, providers of online marketplaces shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to traders that frequently offer products which are non-compliant with this Regulation.

8. Providers of online marketplaces shall cooperate with the market surveillance authorities, with traders and with relevant economic operators to facilitate any action taken to eliminate or, if that is not possible, to mitigate the risks presented by a product that is or was offered online through their services.

Or. en

Justification

The proposed regulation does not address electronic commerce between the EU and third countries. In situations where the consumer or other end-user purchases a product with a digital element from a seller domiciled in a third country through an online marketplace, the seller may not fulfil the definition of importer or distributor laid down in article 3. Products purchased from such parties may not fulfil the cybersecurity requirements. This would infringe the rights of consumers and end-users and provide an unfair competitive advantage to traders and sellers outside the EU.

Amendment 363
Evžen Tošenovský

Proposal for a regulation
Article 18 – paragraph 1

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

Article 10(1) of Regulation (EU) 1025/2012 request one or more European standardisation organisations to draft harmonised standards for the essential requirements set out in Annex I. When preparing the Standardisation Request for this Regulation, the Commission shall aim for maximum harmonisation with existing or imminent international standards for cybersecurity.

Or. en

Amendment 364
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	1a. Products with digital elements and processes put in place by the manufacturer which are in conformity with international standards or parts thereof shall be presumed to be in conformity with the essential requirements covered by those standards or parts thereof, set out in Annex I, where harmonised standards referred to in paragraph 1 of this Article do not exist or where there are undue delays in the standardisation procedure or where the request for harmonised standards by the Commission has not been accepted by the European standardisation organisations.

Or. en

Amendment 365
Evžen Tošenovský, Adam Bielan

Proposal for a regulation
Article 18 – paragraph 2

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

Or. en

Amendment 366
Christophe Grudler, Valérie Hayer

Proposal for a regulation
Article 18 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The Commission is empowered, by means of implementing acts, to specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 ***that can*** be used to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I. Furthermore, ***where applicable, the Commission shall specify if*** a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	4. The Commission is empowered, by means of implementing acts, to specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 ***to*** be used to demonstrate conformity ***of critical products with digital elements*** with the essential requirements or parts thereof as set out in Annex I. Furthermore, ***the issuance of*** a cybersecurity certificate issued under such schemes***, at substantial or high level,*** eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Or. en

Justification

The CRA should be better linked to the Cyber Security Act (CSA) in order to avoid overlaps between the two texts. As the CSA lays down a more rigorous cybersecurity assessment

framework, it should address products presenting a particular cybersecurity risk. As the conformity assessment framework specific to the CRA is less demanding, it should be used to address mass products subjected to the CRA.

Amendment 367
Evžen Tošenovský, Adam Bielan

Proposal for a regulation
Article 19

Text proposed by the Commission	*Amendment*
Article 19	***deleted***
Common specifications	
Where harmonised standards referred to in Article 18 do not exist or where the Commission considers that the relevant harmonised standards are insufficient to satisfy the requirements of this Regulation or to comply with the standardisation request of the Commission, or where there are undue delays in the standardisation procedure or where the request for harmonised standards by the Commission has not been accepted by the European standardisation organisations, the Commission is empowered, by means of implementing acts, to adopt common specifications in respect of the essential requirements set out in Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	

Or. en

Amendment 368
Bart Groothuis

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	***deleted***

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

Or. en

Justification

Deletion because the process proposed circumvents existing best practices around standardization and could enable the Commission to unilaterally impose a standard on industry bypassing all existing best practices and standardization bodies

Amendment 369
Matteo Gazzini, Paolo Borchia, Isabella Tovaglieri, Elena Lizzi, Matteo Adinolfi, Markus Buchheit, Marie Dauchy

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 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	Where harmonised standards referred to in Article 18 do not exist or where the Commission considers that the relevant harmonised standards are insufficient to satisfy the requirements of this Regulation or to comply with the standardisation request of the Commission, or where there are undue delays in the standardisation procedure or where the request for harmonised standards by the Commission has not been accepted by the European standardisation organisations, ***as a last resort*** the Commission is empowered, by

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).	means of implementing acts, 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).

Or. en

Amendment 370
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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 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)***.	Where harmonised standards referred to in Article 18 do not exist or where the Commission considers that the relevant harmonised standards are insufficient to satisfy the requirements of this Regulation or to comply with the standardisation request of the Commission, or where there are undue delays in the standardisation procedure or where the request for harmonised standards by the Commission has not been accepted by the European standardisation organisations, the Commission is empowered, by means of ***delegated acts, in accordance with Article 50***, to adopt common specifications in respect of the essential requirements set out in Annex I ***for products within the scope of this Regulation***.

Or. en

Amendment 371
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Carlos Zorrinho

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. en

Amendment 372
Ignazio Corrao
on behalf of the Verts/ALE Group

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***.

Or. en

Amendment 373
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

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	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.	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. ***When adopting delegated acts, the Commission shall take into account and make sure the administrative burden on micro, small and medium sized enterprises is kept to a minimum.***

Or. en

Amendment 374
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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, ***of the dimension of economic operators with particular regard to micro, small and medium sized enterprises,*** as well as developments encountered in the implementation process of this Regulation.

Or. en

Amendment 375
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	(ca) a European cybersecurity

certification scheme adopted as per Regulation (EU) 2019/881 in accordance with paragraph 4 of Article 18.

Or. en

Amendment 376
Evžen Tošenovský

Proposal for a regulation
Article 24 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. Where, in assessing the compliance of the critical product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer or the manufacturer's authorised representative has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to either of the following procedures:	2. Where, in assessing the compliance of the critical product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer or the manufacturer's authorised representative has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes ***or international standards*** do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to either of the following procedures:

Or. en

Amendment 377
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 24 – paragraph 2 – point b a (new)

Text proposed by the Commission	*Amendment*

(ba) where applicable, a European cybersecurity certification scheme at assurance level 'substantial' or 'high' pursuant to Regulation (EU) 2019/881.

Or. en

Amendment 378
Marc Botenga

Proposal for a regulation
Article 24 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. Where the product is a critical product with digital elements of class II as set out in Annex III, the manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:	3. Where the product is a critical product with digital elements of class II as set out in Annex III, the manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements set out in Annex I by ***acquiring a cybersecurity certificate issued by a European authority, under the European cybersecurity certification scheme and at assurance level "high" as listed in the Regulation (EU) 2019/881. For products with digital elements for which a European cybersecurity certification scheme does not exist or covers them only partially, the manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements set out in Annex I by*** using one of the following procedures:

Or. en

Amendment 379
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 24 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. Where the product is a critical product with digital elements of class II as set out in Annex III, the manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:	3. Where the product is a critical product with digital elements of class II as set out in Annex III, the manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements set out in Annex I ***obtaining a European cybersecurity certificate, under a European cybersecurity certification scheme at assurance level 'high' pursuant to Regulation (EU) 2019/881. Where such European cybersecurity certification schemes do not exist or only cover parts of the critical product with digital elements, the concerned critical product and the processes put in place by the manufacturer shall demonstrate those essential requirements*** by using one of the following procedures:

Or. en

Amendment 380
Marc Botenga

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

Text proposed by the Commission	*Amendment*
	(ba) ENISA shall prepare the missing candidate schemes in order to cover all products listed in Annex III, in accordance with Article 48 of the (EU) 2019/881 Regulation.

Or. en

Amendment 381
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	3a. In accordance with Article 48 of Regulation (EU) 2019/881, the Commission shall request ENISA to prepare the missing candidate schemes with the view of fully covering all the products listed in Annex III.

Or. en

Amendment 382
Ignazio Corrao
on behalf of the Verts/ALE Group

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 (SMEs) when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs. ***The Commission shall take appropriate measures to ensure more accessible and affordable procedures, such as establishing a framework for providing appropriate financial support and guidance for the notified bodies.***

Or. en

Amendment 383
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 24 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Notified bodies shall take into	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.	account the specific interests and needs of ***micro,*** small and medium sized enterprises (SMEs) when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs. ***The Commission shall ensure that appropriate financial support in the regulatory framework of existing Union programmes is allocated to micro, small and medium-sized enterprises, in order to mitigate possible financial burden.***

Or. en

Amendment 384
Evžen Tošenovský

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 ***SMEs*** when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs.

Or. en

Amendment 385
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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	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

reduce those fees proportionately to their specific interests and needs.	fees proportionately to their specific interests and needs.

Or. en

Amendment 386
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 25 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall notify the Commission and the other Member States of conformity assessment bodies authorised to carry out conformity assessments in accordance with this Regulation.	Member States shall notify the Commission and the other Member States of conformity assessment bodies authorised to carry out conformity assessments in accordance with this Regulation. ***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 pursuant to articles 26 to 31.***

Or. en

Amendment 387
Henna Virkkunen, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Adam Jarubas

Proposal for a regulation
Article 28 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. The Commission shall, within 24 months from the entry into force of this Regulation, ensure that there is a sufficient number of notified bodies in the Union to carry out a conformity assessment, in order to avoid bottlenecks and hindrances to market entry.

Or. en

Amendment 388
Evžen Tošenovský

Proposal for a regulation
Article 29 – paragraph 7 – point c

Text proposed by the Commission	*Amendment*
(c) appropriate knowledge and understanding of the essential requirements, of the applicable harmonised standards and of the relevant provisions of Union harmonisation legislation and of its implementing acts;	(c) appropriate knowledge and understanding of the essential requirements ***set out in Annex I***, of the applicable harmonised standards and of the relevant provisions of Union harmonisation legislation and of its implementing acts;

Or. en

Amendment 389
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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

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

Or. en

Amendment 390
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

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	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.	consistent, fair and reasonable terms and conditions, in particular taking into account the interests of ***micro, small and medium sized enterprises*** in relation to fees.

Or. en

Amendment 391
Ignazio Corrao
on behalf of the Verts/ALE Group

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 particular taking into account the interests of ***micro, small and medium enterprises*** in relation to fees.

Or. en

Amendment 392
Evžen Tošenovský

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 SMEs in relation to fees.

Or. en

Amendment 393
Evžen Tošenovský

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. 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.

Or. en

Amendment 394
Evžen Tošenovský

Proposal for a regulation
Article 37 – paragraph 4

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

Or. en

Amendment 395
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Or. en

Justification

Moved below

Amendment 396
Evžen Tošenovský

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 implementation of the reporting obligations pursuant to ***Article*** 11 of this Regulation, the designated market surveillance authorities shall cooperate with ENISA.	3. Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated under Article 58 of Regulation (EU) 2019/881***, competent authorities and CSIRTs designated under Articles 8 and 10 of Directive (EU) 2022/2555*** and exchange information on a regular basis. With respect to the supervision of the implementation of the reporting obligations pursuant to ***Articles 10a and*** 11 of this Regulation, the designated market surveillance authorities shall cooperate with ***CSIRTs and*** ENISA.

Or. en

Amendment 397
Ignazio Corrao
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 41 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 11 of this Regulation, the designated market surveillance authorities shall cooperate with ENISA. The market surveillance authorities may request ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 43, market surveillance authorities may request ENISA to provide non-binding evaluations of compliance of products with digital elements.

Or. en

Amendment 398
Beatrice Covassi, Robert Hajšel, Patrizia Toia, Lina Gálvez Muñoz, Carlos Zorrinho

Proposal for a regulation
Article 41 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and human resources to fulfil their tasks under this Regulation.	6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and human resources***, with appropriate cybersecurity skills, in order*** to fulfil their tasks under this Regulation.

Or. en

Amendment 399
Bart Groothuis

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. Market surveillance authorities may provide guidance and advice to economic operators on the implementation of this Regulation, ***including on non-technical risk factors,*** with the support of the Commission.

Or. en

Justification

The CRA has a missed opportunity to not address the issue of risky vendors, especially in the context of critical infrastructure. While there have been positive developments towards non-binding toolboxes to address specific supply chain security issues related 5G (toolbox) the European Court of Auditors concluded that since the 5G toolbox was adopted, progress has been made to reinforce the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors, but that none of the measures put forward are legally binding, meaning that implementation across the Union is inconsistent at best, and that the Commission has no power to enforce those rules. This should be addressed in the Cyber Resilience Act.

Amendment 400
Evžen Tošenovský

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

Or. en

Amendment 401

Bart Groothuis

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

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

Or. en

Justification

By setting as a main rule that the support period should cover the expected product lifetime, in combination with the transparency about the duration of this expected product lifetime (and therefore support period) proposed below, manufacturers are encouraged to choose a reasonable support period that can be longer than 5 years. This will be monitored by market surveillance authorities.

Amendment 402
Evžen Tošenovský

Proposal for a regulation
Article 41 – paragraph 9 a (new)

Text proposed by the Commission	*Amendment*
	9a. The Commission shall evaluate the reported data, including the for the purpose of report referred to in Article 41(9). Where the reported data suggest an increased level of non-compliance in specific categories of products, the Commission, after consulting the Expert Group and ADCO, may recommend that all surveillance authorities focus closely on the product categories concerned.

Or. en

Amendment 403

Evžen Tošenovský

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) ***for cyber resilience of products with digital elements*** shall be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. This ADCO shall be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of single liaison offices. ***In particular, this ADCO shall exchange best practices and, where relevant, cooperate with Cyber Resilience Expert Group, ENISA, Cooperation Group and CSITs Network.***

Or. en

Amendment 404
Ignazio Corrao
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	11a. Market surveillance authorities shall facilitate the active participation of stakeholders in market surveillance activities, including scientific, research and consumer organisations, by establishing a clear and accessible mechanism to facilitate the voluntary reporting of vulnerabilities, incidents, and cyber threats.

Or. en