European Parliament
2019-2024

Committee on the Internal Market and Consumer Protection

2022/0272(COD)

28.4.2023

AMENDMENTS
57 - 347

Draft opinion
Morten Løkkegaard
(PE742.490v01-00)

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_LegOpinion

Amendment 57
Carlo Fidanza

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 an external network or device*** are designed and developed in accordance with essential requirements laid down in this Regulation. This includes both products that can be connected ***to external networks or device*** physically via hardware interfaces and products that are connected logically, such as via network sockets, pipes, files, application programming interfaces or any other types of software interface. As cybersecurity threats can propagate through various products with digital elements before reaching a certain target, for example by chaining together multiple vulnerability exploits, manufacturers should also ensure the cybersecurity of those products that are only indirectly connected to other devices or networks.

Or. en

Justification

Being the main scope of the CRA related to cyber hacks to networks and products via their external connection the use of terms "connected" or "connectable" should refer only to the external network for connected products (LAN, WAN, or other similar processes facilitating external data exchanges and cloud connectivity) and not the internal network of a machine/vehicle. The latter is used by ECUs (electronic control units) for internal

communication and is generally isolated from external networks through secured dedicated endpoints. (An endpoint is any device that is connected to a network and serves as an entry point to that network -see article 3, point 15).

Amendment 58
Carlo Fidanza

Proposal for a regulation
Recital 7 a (new)

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

Or. en

Amendment 59
Carlo Fidanza

Proposal for a regulation
Recital 7 b (new)

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

Or. en

Justification

Compliance of all products with digital elements is already covered, through the compliance of the original product. A spare part is only replacing an identical component into said product with digital elements. It is necessary to clearly state that spare parts for these products with digital elements do not need a separate certification system.

Amendment 60
Marcel Kolaja
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 cloud computing services and cloud service models, such as SaaS. All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope of that Directive.	(9) This Regulation ensures a high level of cybersecurity of products with digital elements***, 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 their 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 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 61
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Recital 9

Text proposed by the Commission	*Amendment*
(9) This Regulation ensures a high level of cybersecurity of products with digital elements. It does not regulate services, ***such as*** Software-as-a-Service (SaaS)***, except for remote data processing solutions relating to a product with digital elements understood as any*** data processing ***at a distance for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions***. [Directive XXX/XXXX (NIS2)] puts in place cybersecurity and incident reporting requirements for essential and important entities, such as critical infrastructure, with a view to increasing the resilience of the services they provide. [Directive XXX/XXXX (NIS2)] applies to cloud computing services and cloud service models, such as SaaS. All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope	(9) This Regulation ensures a high level of cybersecurity of products with digital elements. It does not regulate services, ***that fall into one or more of the following data processing services models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS),*** Software-as-a-Service (SaaS)***. Those service delivery models represent a specific, pre-packaged combination of IT resources offered by a provider of*** data processing ***service. Three base cloud delivery models are further completed by emerging variations, each comprised of a distinct combination of IT resources***. [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 ***IaaS, PaaS and*** SaaS. All entities providing cloud computing services in the Union that meet or exceed

of that Directive.

the threshold for medium-sized enterprises fall in the scope of that Directive.

Or. en

Amendment 62
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 9 a (new)

Text proposed by the Commission	*Amendment*
	(9 a) Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. Research by the Commission also shows that free and open-source software can contribute between €65 billion to €95 billion to the Union's GDP and that it can provide significant growth opportunities for the European economy. 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 range of different roles in such development models. 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 Union.

Or. en

Amendment 63
Brando Benifei

Proposal for a regulation
Recital 10

Text proposed by the Commission	*Amendment*
(10) In order not to hamper innovation or research, free and open-source software ***developed or*** supplied ***outside*** the course of a commercial activity should ***not*** be covered by this Regulation***. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable***. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.	(10) ***Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. Research by the Commission also shows that free and open-source software can contribute between €65 billion to €95 billion to the Union's GDP and that it can provide significant growth opportunities for the European economy.*** In order not to hamper innovation or research, ***only*** free and open-source software supplied ***in*** the course of a commercial activity should be covered by this Regulation. 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 does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise***, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the

security, compatibility or interoperability of the software. ***Neither the collaborative development of free and open-source software components nor making them available on open repositories should constitute a placing on the market or putting into service. The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity.***

Or. en

Amendment 64
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 18 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 Union.

Or. en

Amendment 65
Marcel Kolaja
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 Regulation.*** 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 ***software (such as an App Store)***, or by the use of personal data for reasons other than exclusively for improving the security,

compatibility or interoperability of the software. ***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 66
Karen Melchior, Sandro Gozi, Svenja Hahn

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) ***Research by the Commission shows that Open Source software contributes between €65 billion to €95billion to the Union's GDP, and provides significant growth opportunities for the Union economy. Therefore,*** in order not to hamper innovation or research, ***freeware*** and open-source software supplied outside the course of a commercial activity should not be covered by this Regulation. 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 ***the core functionality of which relies on other services*** which the manufacturer monetises, 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

The addition of freeware means that developers of propitiatory software that is provided free of charge shall not be subject to liability. Change in what can be defined as "commercial activity" so as to exclude open-source software repositories provided as a public good while including the intended targets (Android Operating System, Propitiatory services with open source clients etc..)

Amendment 67
Karen Melchior, Sandro Gozi, Svenja Hahn

Proposal for a regulation
Recital 10 a (new)

Text proposed by the Commission	*Amendment*
	(10 a) Due to the permissive nature of open-source licences, open-source software can be used as a component in products without need for the consent or knowledge of the original author, allowing for manufacturers to build new products and services quickly, however open-source software developers are not compensated for this use and often work on the software in their free time. Therefore, when a manufacturer uses open-source software as a component in a product, they should be subject to the obligations of manufacturers for that component, unless otherwise agreed through the provision of commercial technical support either by the developer or a third-party.

Or. en

Justification

In software development, use of unvetted software libraries of part of products without review has become a serious issue in recent years, leading to security flaws in numerous products. This amendment ensures open-source developers are not burdened with the responsibilities of manufacturers, and that manufacturers of products which use open source components do their due diligence.

Amendment 68
Brando Benifei

Proposal for a regulation
Recital 10 a (new)

Text proposed by the Commission	*Amendment*
	(10 a) Free and open-source software is developed, maintained, and distributed via online platforms. In contrast to app stores that make products available, these entities play an important research and development role. As such, package managers, code hosting, and collaboration platforms do not make software products available on the market as distributors within this Regulation.

Or. en

Amendment 69
Karen Melchior, Sandro Gozi, Svenja Hahn

Proposal for a regulation
Recital 10 b (new)

Text proposed by the Commission	*Amendment*
	(10 b) Public open-source code and software repositories allow developers to access a wide range of resources for software development, and allow for developers to share their code with the wider open-source community. These repositories operate as a public good, and therefore should not be considered as providers, manufacturers, importers or distributors, nor should their activity be considered as commercial within the meaning of this Regulation.

Or. en

Justification

Public open-source code and software repositories store code and software from various developers which is accessible to developers all over the world for free, and are at the heart of the Open Source ecosystem. They should not be subject to this regulation as they do not control all the code on their repositories. Fundraising activities that ensure these platforms can continue to provide access to code for free, such as offering coding classes or selling tickets to conferences, should not be considered as commercial activities.

Amendment 70
Adam Bielan

Proposal for a regulation
Recital 11 a (new)

Text proposed by the Commission	*Amendment*
	(11 a) According to the WTO Agreement on Technical Barriers to Trade, when technical regulations are necessary and relevant international standards exist, WTO Members should use those standards as the basis for their own technical regulations. It is important to avoid duplication of work among standardisation organizations, as international standards are intended to facilitate the harmonization of national and regional technical regulations and standards, thereby reducing non-tariff technical barriers to trade. Given that cybersecurity is a global issue, the Union should strive for maximum alignment. To achieve this objective, the standardization request for this Regulation, as set out in Article 10 of Regulation 1025/2012, should seek to reduce barriers to the acceptance of standards by publishing their references in the Official Journal of the EU, in accordance with Article 10 (6) of Regulation 1025/2012.

Or. en

Justification

The WTO Agreement specifies the superiority of international standards over regional or

national standards; however, it allows for legitimate deviations based on fundamental climatic or geographical factors, or fundamental technological challenges, as per Article 2.4 of the WTO Agreement on Technical Barriers to Trade. Since cybersecurity threats are of a global nature, such exemptions do not apply in this case. Hence, existing international standards should be used wherever possible as harmonised standards, with minimal deviation.

Amendment 71
Adam Bielan

Proposal for a regulation
Recital 11 b (new)

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

Or. en

Amendment 72
Carlo Fidanza

Proposal for a regulation
Recital 13 a (new)

Text proposed by the Commission	*Amendment*
	(13 a) Agricultural and forestry vehicles in scope of Regulation (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

Justification

So far agricultural and forestry vehicles do not have cybersecurity requirements embedded in their type approval legislation (Regulation 167/2013) and thus will have to comply with this regulation. It should be specified that CRA and its horizontal requirements will be the reference for these vehicles. Double regulation on the same topic should be avoided.

Amendment 73
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Recital 16 a (new)

Text proposed by the Commission	*Amendment*
	(16 a) Without prejudice to the rules set out in Directive 85/374/EEC, manufacturers should also be liable for the damages suffered by consumers that are caused by their infringement of the legal obligations and cybersecurity requirements set out in this Regulation. Such compensation should be in accordance with the rules and procedures set out in the applicable national law and without prejudice to other possibilities for redress available under consumer protection rules.

Or. en

Justification

The proposal fails to establish any right to redress or compensation for affected users. The CRA should be aligned with the latest EU digital legislation such as the Digital Services Act and the Digital Market Act which contain provisions to ensure that consumers have clear rights and effective means to seek redress in case of non-compliance with any of the obligations set out in these Regulations. Affected consumers should have the right to seek adequate redress and compensation against any damage or loss suffered due to an infringement of the obligations and requirements under the CRA.

Amendment 74
Arba Kokalari

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 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	(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.

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. ***ENISA should publish and maintain a known exploited vulnerability catalogue, as an authoritative source of vulnerabilities exploited. Manufacturers should monitor the catalogue and notify any listed vulnerability found in their product. Active exploitation in this context does not include scanning, security research exploits or Proofs of Concept.***

Or. en

Amendment 75
Adam Bielan, Kosma Złotowski

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***	(19) Certain tasks provided for in this Regulation should be carried out by the relevant Computer Security Incident Response Teams (CSIRTs) or the relevant ***market surveillance authority. In particular, CSIRTs should receive notification from manufacturers of actively exploited vulnerabilities having a significant impact on products with digital elements, as well as incidents having a significant impact on the security of those products. CSIRTs or*** the relevant market surveillance ***authority, should submit to ENISA information on notifications provided such information is relevant for the coordinated response to large-scale cybersecurity incidents. For the purpose of this Regulation, an incident shall be considered to be significant if (i) it has***

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.***

caused or is capable of causing severe operational disruption of the production or the development, build and distribution environment for the manufacturer concerned, that would impact the security of a product; or (ii) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive ***(EU) 2022/2555***. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised.

Or. en

Amendment 76
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Recital 20

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

on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.

unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.

Or. en

Amendment 77
Adam Bielan, Kosma Złotowski

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 increased because of***	(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 ***materially alters the core function of a product***, the modification should be considered as substantial. For example, software updates or repairs could be assimilated to maintenance operations provided that they do not ***introduce substantial changes to the functions or cybersecurity architecture of*** a product already placed on the market***, that change the level of hazard or risk*** for which the product ***was*** assessed***.***

the software update.

Or. en

Amendment 78
Arba Kokalari

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 increased because of the software update.	(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. 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 level of risk has ***significantly*** increased because of the software update.

Or. en

Amendment 79
Marcel Kolaja
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 increased because of the software update.	(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 assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.

Or. en

Amendment 80
Arba Kokalari

Proposal for a regulation
Recital 23

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

Or. en

Amendment 81
Adam Bielan, Kosma Złotowski

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	(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, it is appropriate that the compliance of the product with digital elements is verified and that, where

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.

applicable, ***the*** conformity assessment ***updated***. Where applicable, if the manufacturer undertakes a conformity assessment involving a third party, changes that might lead to substantial modifications should be notified to the third party. ***The subsequent conformity assessment should address the changes that lead to the new assessment, unless these changes have significant impact on the conformity of other parts of the product.***

Or. en

Amendment 82
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 24 a (new)

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

Or. en

Amendment 83
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Recital 24 a (new)

Text proposed by the Commission	*Amendment*
	(24 a) Manufacturers should clearly differentiate between security and functionality updates, and ensure that they are provided separately in a clear and transparent way. Manufacturers should therefore provide these updates separately, unless technically unfeasible. Manufacturers should provide consumers with adequate information on the motive behind each update and its foreseen impact on the product, as well as a clear and easy-to-use opt-out mechanism.

Or. en

Justification

The CRA proposal should oblige manufacturers to differentiate between security updates (to provide devices with enhanced security, including security patches) and corrective or functionality updates (to 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.

Amendment 84
Marcel Kolaja
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	(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. 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***.	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 85
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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	(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 reasonably foreseen misuse caused by a cyberattack***. 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

XXX/ XXXX (NIS2)], or for the performance of critical or sensitive functions, such as processing of personal data.	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.

Or. en

Justification

The definition of cybersecurity risk must be broader and more comprehensive. Besides the protection of the physical integrity, a risk assessment must always consider potential threats to fundamental rights and the safety or integrity of an individual. In case of consumer products, they should clearly be considered critical products of higher risk, when either their intended use or reasonably foreseen misuse caused by a cyberattack creates a risk of harm to their health and safety, or a risk of adverse impact on fundamental rights (including privacy and data protection) of the users.

Amendment 86
Adam Bielan

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 environments ***of high criticality***, and therefore should undergo a stricter conformity assessment procedure.

Or. en

Justification

Purpose: consistency through the legislative text

Amendment 87
Marcel Kolaja
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 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].	(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 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 88
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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 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].	(28) This Regulation addresses cybersecurity risks in a targeted manner***, including other risks related to their intended use or reasonably foreseen misuse of*** products with digital elements ***caused by a cyberattack. Therefore,*** safety risks ***related to the cybersecurity functions of products with digital elements shall fall within the scope of this Regulation. Other risks which*** are not related to cybersecurity should continue to be regulated by other relevant Union product legislation. If no other Union harmonisation legislation is applicable, they should be subject to Regulation [General Product Safety Regulation]. Therefore, in light of the targeted nature of this Regulation, as a derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] should apply to products with digital elements with respect to safety risks not covered by this Regulation, if those products are not subject to specific requirements imposed by other Union harmonisation legislation within the meaning of [Article 3, point (25) of the General Product Safety Regulation].

Or. en

Justification

Products with digital elements may pose safety risks in connection with their cybersecurity functions. Safety risks triggered by cybersecurity breaches differ from the objectives set out in

the CRA or GPSR. Based on the product's intended use or reasonably foreseen misuse caused by a cyberattack, malicious third parties may create a clear risk of harm to the health and safety, or a risk of adverse impact on fundamental rights (including privacy and data protection) of the users.

Amendment 89
Andreas Schwab, Deirdre Clune

Proposal for a regulation
Recital 29

Text proposed by the Commission	*Amendment*
(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation[27] [the AI Regulation] which fall within the scope of this Regulation should comply with the essential requirements set out in this Regulation. When those high-risk AI systems fulfil the essential requirements of this Regulation, they should be deemed compliant with the cybersecurity requirements set out in Article [Article 15] of Regulation [the AI Regulation] in so far as those requirements are covered by the EU declaration of conformity or parts thereof issued under this Regulation. As regards the conformity assessment procedures relating to the essential cybersecurity requirements of a product with digital elements covered by this Regulation and classified as a high-risk AI system, the relevant provisions of Article 43 of Regulation [the AI Regulation] should apply as a rule instead of the respective provisions of this Regulation. ***However,*** this rule should ***not result in reducing the necessary*** level of assurance for critical products with digital elements covered by this Regulation. ***Therefore, by way of derogation from this rule, high-risk*** AI systems that fall within the scope of ***the Regulation*** [the AI Regulation] and are also qualified as critical products with digital elements ***pursuant to*** this Regulation ***and to which*** the conformity	(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation[27] [the AI Regulation] which fall within the scope of this Regulation should comply with the essential requirements set out in this Regulation. When those high-risk AI systems fulfil the essential requirements of this Regulation, they should be deemed compliant with the cybersecurity requirements set out in Article [Article 15] of Regulation [the AI Regulation] in so far as those requirements are covered by the EU declaration of conformity or parts thereof issued under this Regulation. As regards the conformity assessment procedures relating to the essential cybersecurity requirements of a product with digital elements covered by this Regulation and classified as a high-risk AI system, the relevant provisions of Article 43 of Regulation [the AI Regulation] should apply as a rule instead of the respective provisions of this Regulation. This rule should ***create a high*** level of assurance for critical products with digital elements covered by this Regulation. ***For high risk*** AI systems that fall within the scope of [the AI Regulation] and are also qualified as critical products with digital elements ***under*** this Regulation***, the responsible sectoral notified body should be responsible for conducting*** the conformity assessment ***under this***

assessment ***procedure based on internal control referred to in Annex VI of the*** Regulation ***[the AI Regulation] applies, should be subject to the*** conformity assessment ***provisions of this Regulation in so far as the essential requirements of this Regulation are concerned. In this case, for all the other aspects covered by Regulation [the AI Regulation] the respective provisions on conformity assessment based on internal control set out in Annex VI to Regulation [the AI Regulation] should apply***.	Regulation ***and lead the administrative process such that economic operators can address their request for*** conformity assessment ***to a single regulatory body***.
[27] Regulation [the AI Regulation].	[27] Regulation [the AI Regulation].

Or. en

Justification

The goal of the CRA and AIA is to create a framework for secure and trustworthy products. To ensure a fully harmonized single market approach in line with the NLF, economic operators should not have to undergo several conformity assessments, but a single one. Instead, economic operators should be able to fulfil their conformity assessment requirements with their existing regulatory body such as a notified body. The sectoral regulatory body should lead the conformity assessment process.

Amendment 90
Marcel Kolaja
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,	***deleted***

sections 1.1.9 and 1.2.1] of the Regulation [Machinery Regulation proposal], as regards protection against corruption and safety and reliability of control systems in so far as the compliance with those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.

Or. en

Amendment 91
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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 requirements is demonstrated by the EU declaration of conformity issued under this Regulation.	(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 requirements is demonstrated by the EU declaration of conformity issued under this Regulation ***without prejudice to products with digital elements, which are also machinery products that fall within the categories listed in Annex I of Regulation [Machinery Regulation proposal], being subject to the specific conformity assessment procedure as required by Article 21(2) and (3) of Regulation [Machinery Regulation proposal]***.

Or. en

Justification

The protection objectives, the requirements and, most importantly, the conformity assessment procedures of the CRA and the Machinery Products Regulation differ significantly. Therefore, the presumption of conformity - by applying the CRA requirements to demonstrate conformity with the cybersecurity requirements of the Machinery Products Regulation - should be clarified.

Amendment 92
Marcel Kolaja
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 93
Adam Bielan

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 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. ***Products with digital elements shall be either placed on the market delivered without any known critical or high severity exploitable vulnerabilities or manufacturers shall provide based on a risk assessment the appropriate impact mitigation such as by security updates before the product is put into service for the first time.***

Or. en

Justification

A risk-based approach should be adopted when dealing with vulnerabilities, as some may present negligible risks that do not result in incidents. Mandating manufacturers to address all vulnerabilities, irrespective of their impact and cost, would be impractical and

burdensome. It may also lead to the unavailability or removal of essentially secure products, causing unnecessary disruption to the market. Instead, manufacturers should be required to document and assess any vulnerabilities in their products, which are not significant at the time of placement in the market.

Amendment 94
Arba Kokalari

Proposal for a regulation
Recital 32

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

Or. en

Amendment 95
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 32 a (new)

Text proposed by the Commission	*Amendment*
	(32 a) 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 96
Adam Bielan, Kosma Złotowski

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	***deleted***

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.

Or. en

Justification

Recital duplicates the NIS 2 provisions.

Amendment 97
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

Proposal for a regulation
Recital 34 a (new)

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

Or. en

Justification

To be able to report on exploitable vulnerabilities manufacturers need an authoritative list.

Amendment 98
Arba Kokalari

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) Manufacturers should also report to ENISA any incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive [Directive XXX/XXXX (NIS2)] for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where 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.	***deleted***

Or. en

Amendment 99
Marcel Kolaja
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	(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.

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. ***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 100
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) Manufacturers should also report to	(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.

relevant CSIRTs or, where applicable the relevant market surveillance authority, any incident having ***a significant*** impact on the security of the product with digital elements. In order to ensure that users can react quickly to incidents having ***a significant*** impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident 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 101
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Recital 38

Text proposed by the Commission	*Amendment*
(38) In order to facilitate assessment of conformity with the requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements which are in conformity with harmonised standards, which translate the essential requirements	(38) In order to facilitate assessment of conformity with the requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements which are in conformity with harmonised standards, which translate the essential requirements

of this Regulation into detailed technical specifications, and which are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council[29] . Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements of this Regulation.	of this Regulation into detailed technical specifications, and which are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council[29] . Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements of this Regulation. ***The standardisation process should ensure a balanced representation of interests and effective participation of civil society stakeholders, including consumer organisations.***
[29] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).	[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).

Or. en

Justification

Technical standards must not go beyond the implementation of mere technical aspects and enter in areas of public policy and law which require a certain level of interpretation. Moreover, civil society and consumers' interests are not sufficiently represented at national, European and international standardisation bodies.

Amendment 102
Marcel Kolaja
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 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	(45) As a general rule ***the requirements for*** the conformity assessment of products with digital elements should ***be risk-based and to that regard in many cases the assessment could*** be carried out by the manufacturer under its own responsibility following the procedure based on Module A of Decision 768/2008/EC. The manufacturer should retain flexibility to choose a stricter conformity assessment procedure involving a third-party. If the product is classified as a critical product of class I, additional assurance is required to demonstrate conformity with the essential requirements set out in this Regulation. The manufacturer should apply harmonised standards, 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

always involve a third party.

products classified as critical class II products, the conformity assessment should always involve a third party.

Or. en

Amendment 103
Arba Kokalari

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	(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 or cybersecurity certification schemes under Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act, if it wants to carry out the conformity assessment under its own responsibility (module A). If the manufacturer does not apply such harmonised standards or cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party. Taking into account the administrative burden on manufacturers and the fact that 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

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.	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 104
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Recital 56 a (new)

Text proposed by the Commission	*Amendment*
	(56 a) In order for SMEs to be able to cope with the new obligations imposed by this Regulation, the Commission should provide them with relevant guidelines.

Or. en

Amendment 105
Arba Kokalari

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	(62) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 of the Treaty

should be delegated to the Commission in respect of updates to the list of critical products in Annex III and specifying the definitions of the these product categories. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential ***mandating of*** certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[33] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

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

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 ***voluntary*** certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making 33 . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

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

Or. en

Amendment 106
Arba Kokalari

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 (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] .	(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***,*** ***based on industry best practices***, specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts therefore as set out in Annex I of this Regulation, adopt common specifications in respect of the essential requirements set out in Annex I, lay down technical specifications for pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use, decide on corrective or restrictive measures at Union level in exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[34] .
[34] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).	[34] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

Or. en

Amendment 107
Marcel Kolaja
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 108
Arba Kokalari

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 [***48*** months] from its entry into force, with the exception of the reporting obligations concerning ***known*** exploited vulnerabilities and ***significant*** incidents, which should apply [***24*** months] from the entry into force of this Regulation

Or. en

Amendment 109
Arba Kokalari

Proposal for a regulation
Recital 71 a (new)

Text proposed by the Commission	*Amendment*
	(71 a) The Commission shall present easy-to-understand guidelines for businesses with the requirements of this Regulation. When developing such guidelines, the Commission should take into consideration needs of SMEs so as to keep administrative and financial burdens to a minimum while facilitating their compliance with this Regulation. The Commission should consult relevant stakeholders, with expertise in the field of cybersecurity.

Or. en

Amendment 110
Arba Kokalari

Proposal for a regulation
Recital 71 b (new)

Text proposed by the Commission	*Amendment*
	(71 b) Where third party assessment is mandated, such assessment should take into account: the similarity of products with digital elements by accepting one product as representative of a family or category of products for assessment purposes due to them having equitable hardware and/or software; reciprocity to eliminate duplication by accepting of other entities' assessments or certification (e.g. recognition of assessments from qualified bodies outside the Union; reuse of certifications); deltas in order to only focus on additional requirements not

covered by other entities' assessments and not reassessing the whole set; attestation in order to accept assessments from the manufacturer for certain aspects of the wider third-party assessment; and maintenance to allow certain changes or software updates to the product without requiring reassessment. In particular, software updates that do not weaken the security posture of the product should not be considered as justifiable to require reassessment.

Or. en

Amendment 111
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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

Text proposed by the Commission	*Amendment*
This Regulation lays down:	***The objective of this Regulation is to provide for a high level of consumer protection by protecting the confidentiality, integrity and availability of information in products with digital elements.*** This Regulation lays down:

Or. en

Amendment 112
Marcel Kolaja
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	(d) rules on ***market monitoring,*** market

enforcement of the above-mentioned rules and requirements.	surveillance and enforcement of the above-mentioned rules and requirements.

Or. en

Amendment 113
Adam Bielan, Kosma Złotowski

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 network.

Or. en

Justification

The concept of a network already covers situations where a device connect to the network via other device. Proposed text includes offline setups.

Amendment 114
Carlo Fidanza

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.

Or. en

Justification

Being the main scope of the CRA related to cyber hacks to networks and products via their external connection the use of terms "connected" or "connectable" should refer only to the external network for connected products (LAN, WAN, or other similar processes facilitating external data exchanges and cloud connectivity) and not the internal network of a machine/vehicle. The latter is used by ECUs (electronic control units) for internal communication and is generally isolated from external networks through secured dedicated endpoints.(An endpoint is any device that is connected to a network and serves as an entry point to that network -see article 3, point 15).

Amendment 115
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
	(c a) Regulation (EU) 2022/2554;

Or. en

Amendment 116
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
	(c b) Directive (EU) 2022/2555.

Or. en

Amendment 117
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	3 a. 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 118
Arba Kokalari

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

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

Or. en

Amendment 119
Carlo Fidanza

Proposal for a regulation
Article 2 – paragraph 5 – subparagraph 1 (new)

Text proposed by the Commission	*Amendment*
	6. 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

Justification

Being the main scope of the CRA related to cyber hacks to networks and products via their external connection the use of terms "connected" or "connectable" should refer only to the external network for connected products (LAN, WAN, or other similar processes facilitating external data exchanges and cloud connectivity) and not the internal network of a machine/vehicle. The latter is used by ECUs (electronic control units) for internal communication and is generally isolated from external networks through secured dedicated endpoints.(An endpoint is any device that is connected to a network and serves as an entry point to that network -see article 3, point 15).

Amendment 120
Karen Melchior, Sandro Gozi, Svenja Hahn

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

Text proposed by the Commission	*Amendment*
	5 a. This Regulation does not apply to freeware and open-source software unless:
	(a) the developer or a third-party has agreed to the provision of technical support services, either with a user, or with a manufacturer who wishes to use the software as a component in their own products.
	(b) the software is provided in the course of commercial activity, either by:
	(i) charging a price for a product;
	(ii) providing a software platform reliant on other services which the manufacturer monetises;
	(iii) using personal data generated by the software for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

Or. en

Justification

Given how large a role open source software plays in software development today, it should be included as an article and not just as a recital for the sake of clarity.

Amendment 121
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
	5 a. 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 122
Carlo Fidanza

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

Text proposed by the Commission	*Amendment*
	5 a. 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

Justification

Compliance of all products with digital elements is already covered, through the compliance of the original product. A spare part is only replacing an identical component into said product with digital elements. It is necessary to clearly state that spare parts for these

products with digital elements do not need a separate certification system.

Amendment 123
Marcel Kolaja
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 components to be placed on the market separately;	(1) 'product with digital elements' means any software or hardware product its ***ancillary services, including*** remote data processing solutions, ***and*** software or hardware components to be placed on the market separately;

Or. en

Amendment 124
Adam Bielan, Kosma Złotowski

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 125
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
	(1 a) 'partly completed products with digital elements' means an assembly which cannot in itself function so as to perform a specific application and which is only intended to be incorporated into or assembled with a product with digital elements or other partly completed product with digital elements, thereby forming a product with digital elements;

Or. en

Amendment 126
Adam Bielan, Kosma Złotowski

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

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

Or. en

Amendment 127
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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

Text proposed by the Commission	*Amendment*
	(4 a) 'consumer' means any natural person who, under the circumstances

regulated by this Regulation, is acting for purposes which are outside their trade, business, craft or profession;

Or. en

Justification

The CRA should also include safeguards for consumers. To this end, 'consumer' must be defined in alignment with the EU consumer acquis.

Amendment 128
Adam Bielan, Kosma Złotowski

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 the Internet websites***;

Or. en

Amendment 129
Karen Melchior, Sandro Gozi, Svenja Hahn

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

Text proposed by the Commission	*Amendment*
	(6 a) 'freeware' means proprietary software that is provided at no cost to the user, but cannot be distributed, studied, changed, improved, integrated into other products or provided as a service without the consent of the author;

Or. en

Justification

A definition of freeware for the purposes of exempting it

Amendment 130
Karen Melchior, Sandro Gozi, Svenja Hahn

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

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

Or. en

Justification

A definition of open source software for the purpose of exempting it

Amendment 131
Carlo Fidanza

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

Justification

The inclusion of "radio waves" in the definition leads to ambiguity as the word physical

implies it is not wireless.

Amendment 132
Marcel Kolaja
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 133
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 3 – paragraph 1 – point 23

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

Or. en

Amendment 134
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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

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

Or. en

Justification

Clarification and alignment of definitions with Regulation (EU) 2019/1020 on market surveillance and compliance of products.

Amendment 135
Adam Bielan, Kosma Złotowski

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***
	(This amendment applies throughout the text.)

Or. en

Justification

The idea of 'reasonably foreseeable misuse' links to the traditional products and given the broad scope of this regulation as well as limitless design options of the software it introduces impossible to comply with obligation, open to subjective interpretation that will differ between the Member States and rely on accidental circumstances.

Amendment 136
Adam Bielan, Kosma Złotowski

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 ***has material impact on the core function*** of the product with digital elements;

Or. en

Amendment 137
Arba Kokalari

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

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

Or. en

Amendment 138
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
(39) ‘actively exploited vulnerability’ means a vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner;	(39) ‘actively exploited vulnerability’ means a ***patched*** vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner;

Or. en

Amendment 139
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

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

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

Or. en

Amendment 140
Arba Kokalari

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

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

Or. en

Amendment 141
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin

Proposal for a regulation
Article 4 – paragraph 1

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

Or. en

Amendment 142
Arba Kokalari

Proposal for a regulation
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall not impede, for the matters covered by this Regulation, the making available on the market of	1. Member States shall not impede, for the matters covered by this Regulation, the making available on the market of

products with digital elements which comply with this Regulation.	products with digital elements ***or partly completed products with digital elements*** which comply with this Regulation.

Or. en

Amendment 143
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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. 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 ***provided that the product is used exclusively for exhibition purposes within the course of such event and that a visible sign clearly indicates that it does not comply with this Regulation***.

Or. en

Amendment 144
Marcel Kolaja
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 145
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

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

Or. en

Amendment 146
Arba Kokalari

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

Or. en

Amendment 147
Marcel Kolaja
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 148
Adam Bielan, Kosma Złotowski

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 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 149
Marcel Kolaja
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 150
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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

Or. en

Justification

The CRA proposal should oblige manufacturers to differentiate between security updates (to provide devices with enhanced security, including security patches) and corrective or functionality updates (to 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.

Amendment 151
Arba Kokalari

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 ***48 months after the start of application of this Regulation and every 5 years thereafter***. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into account:

Or. en

Amendment 152
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

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

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

Or. en

Justification

Industrial settings should not by default be considered higher risk than other settings.

Amendment 153
Arba Kokalari

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

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

Or. en

Amendment 154
Arba Kokalari

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 155
Marcel Kolaja
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 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 ***6*** months since the entry into force of this Regulation].

Or. en

Amendment 156
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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 ***6*** months since the entry into force of this Regulation].

Or. en

Justification

To ensure the proper application of the CRA proposal without undue delays, the Commission should define the product categories falling under the scope of the CRA proposal as swiftly as possible. There can be no justification for further delaying the application of these rules for yet another year.

Amendment 157
Marcel Kolaja
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 158
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini

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(3)***.

Or. en

Justification

Critical products meeting the criteria set out in Article 6 should always undergo an independent third-party assessment. Therefore, the option of self-assessment proposed for class I products should be deleted. A self-assessment by the manufacturer cannot provide the necessary assurance level that is required and equally cannot provide the necessary level of trust for consumers and users. Potential conflicts of interests must be excluded when the product is associated with high risks.

Amendment 159
Adam Bielan, Kosma Złotowski

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 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:	***deleted***
(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 160
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
5. The Commission is empowered to	5. The Commission is empowered to

adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers ***shall be required to*** obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:	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 ***may*** obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:

Or. en

Amendment 161
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation] where products with digital elements ***are not subject to specific requirements laid down in other Union harmonisation legislation*** within the ***meaning of [Article 3, point (25) of the General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation*** [General Product Safety Regulation] shall ***apply to those products with respect to*** safety ***risks not covered by*** this Regulation.	Products with digital elements ***as defined and falling*** within the ***scope of*** [General Product Safety Regulation] shall ***be deemed as complying with the cybersecurity requirements for the purpose of [Article 5 of General Product*** Safety ***Regulation] if they comply with the requirements of*** this Regulation.

Or. en

Amendment 162
Arba Kokalari

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation] ***where*** products with digital elements ***are not subject to specific requirements laid down in other Union harmonisation legislation*** within the meaning of ***[***Article ***3, point (25) of*** the General Product Safety Regulation], ***Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] shall apply to those products with respect to safety risks not covered by*** this Regulation.	***Products falling under the*** Regulation [General Product Safety Regulation] ***which are*** products with digital elements within the meaning of ***this Regulation shall be deemed to be in conformity with*** Article ***5a-1(h) of*** the General Product Safety Regulation], ***when they comply with the requirements of*** this Regulation.

Or. en

Amendment 163
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

Proposal for a regulation
Article 8 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Products with digital elements classified as high-risk AI systems in accordance with Article [Article 6] of Regulation [the AI Regulation] which fall within the scope of this Regulation, and fulfil the essential requirements set out in Section 1 of Annex I of this Regulation, and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2	1. ***Products with digital elements or partly completed*** products with digital elements classified as high-risk AI systems in accordance with Article [Article 6] of Regulation [the AI Regulation] which fall within the scope of this Regulation, and fulfil the essential requirements set out in Section 1 of Annex I of this Regulation, and where the processes put in place by the manufacturer are compliant with the

of Annex I, shall be deemed in compliance with the requirements related to cybersecurity set out in Article [Article 15] of Regulation [the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.

essential requirements set out in Section 2 of Annex I, shall be deemed in compliance with the requirements related to cybersecurity set out in Article [Article 15] of Regulation [the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.

Or. en

Amendment 164
Arba Kokalari

Proposal for a regulation
Article 8 – paragraph 2

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

Or. en

Amendment 165
Andreas Schwab, Deirdre Clune

Proposal for a regulation
Article 8 – paragraph 2

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

Or. en

Justification

The AI regulation is a moving target as regards the applicable provisions on the conformity assessments for high-risk AI. One important goal of the undersigned is to ensure that per harmonized product legislation to which the CRA and AIA high-risk provisions apply, companies only file one request for conformity assessment with the notified body under that harmonized product legislation.

Amendment 166
Andreas Schwab, Deirdre Clune

Proposal for a regulation
Article 8 – paragraph 3

Text proposed by the Commission	*Amendment*
3. By derogation from paragraph 2,	***deleted***

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

Or. en

Justification

The deletion is indicative of the objective only. The goal is to ensure that also critical products in the meaning of the CRA which are high risk AI do not have to undergo more than one conformity assessment.

Amendment 167
Arba Kokalari

Proposal for a regulation
Article 8 – paragraph 3

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

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

Or. en

Amendment 168
Arba Kokalari

Proposal for a regulation
Article 9 – paragraph 1

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

Or. en

Amendment 169
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

Proposal for a regulation
Article 9 – paragraph 1

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

Or. en

Amendment 170
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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

Text proposed by the Commission	*Amendment*
	By derogation from paragraph 1, products with digital elements which are also machinery products that fall within the categories listed in Annex I of Regulation [Machinery Regulation proposal], shall be subject to the specific conformity assessment procedures as required by Article 21(2) and (3) of Regulation [Machinery Regulation proposal].

Or. en

Justification

The protection objectives, the requirements and, most importantly, the conformity assessment procedures of the CRA and the Machinery Products Regulation differ significantly. Therefore, the presumption of conformity - by applying the CRA requirements to demonstrate conformity with the cybersecurity requirements of the Machinery Products Regulation - should be clarified.

Amendment 171
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 18 months from placing a software on the market.

Or. en

Amendment 172
Adam Bielan, Kosma Złotowski

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 ***take reasonable measures to*** ensure 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 173
Carlo Fidanza

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

Justification

In order to make article 10 consistent with the proposed clarifications to article 2 – scope, as well as new recital 7bis.

Amendment 174
Brando Benifei

Proposal for a regulation
Article 10 – paragraph 3

Text proposed by the Commission	*Amendment*
3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject	3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V ***in a manner suitable for distribution of that component and which does not limit the***

to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.	***options for further making available of the component***. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.

Or. en

Amendment 175
Marcel Kolaja
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 security of the product with digital elements.	4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. ***It falls upon the manufacturer to*** ensure that such components do not compromise the security of the product with digital elements***, in particular in the case of open source software that have not been placed on the market by charging a price or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software***. ***The due diligence obligation can be considered fulfilled if all components have been already deemed compliant and the CE marking has been affixed to them as appropriate.***

Or. en

Amendment 176
Adam Bielan, Kosma Złotowski

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. They shall ***take reasonable measures to*** ensure that such components do not compromise the security of the product with digital elements.

Or. en

Amendment 177
Carlo Fidanza

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*** the 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

Justification

Many complex industrial machineries have a very long lifecycle (20 years+). Therefore, keeping these product cybersecure by means of software updates could only be possible up to a period of maximum 10 years, because after some years the new & more advanced software updates would demand significant hardware changes not compatible with the original machinery. 10 years is the real maximum. After, there would be an issue of compatibility or unavailability of the required updates.

Amendment 178
Marcel Kolaja
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, 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 the expected product lifetime is shorter than 5 years, and the manufacturer is unable to continue to ensure that vulnerabilities of the product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I, it shall publish the source code under free and open source license.***

Or. en

Amendment 179
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria

Grapini, Brando Benifei

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.

Or. en

Justification

Article 10(6) currently caps the manufacturers' obligation for 'continuous conformity' at a maximum of five years, regardless of the actual lifespan of the products. We propose a more proportional approach that takes into consideration the specificities of the usage and expected lifespans of all the types of connected products which this regulation is designed to cover. Products should therefore be secure during a minimum period of time which must correspond to the expected lifetime of the actual product, based on its intended use and the legitimate expectations of consumers.

Amendment 180
Arba Kokalari

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	When placing a product with digital elements on the market, and for the expected product lifetime ***at the time of placing that product on the market*** or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the

of Annex I.	essential requirements set out in Section 2 of Annex I.

Or. en

Amendment 181
Adam Bielan, Kosma Złotowski

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 a period of five years from the placing of the product on the market ***or a*** shorter ***period, appropriate to the type and specificity of product***, 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.

Or. en

Amendment 182
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	Manufacturers shall set out the expected product lifetime considering the reasonable expectations of consumers regarding the functionality and intended purpose of the product, and the provision of security and functionality updates.

Or. en

Amendment 183
Marcel Kolaja
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 184
Adam Bielan

Proposal for a regulation
Article 10 – paragraph 9

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

such improvements periodically for future product generations. 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 185
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	9 a. 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 186
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	10 a. Manufacturers shall indicate the expected product lifetime in a clear and understandable manner. Where applicable, manufacturers shall also specify the expected product lifetime on the packaging of the product with digital elements.

Or. en

Amendment 187
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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, 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 188
Marcel Kolaja
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	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***.	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, ***or publish the source code under free and open source license with this information in order to encourage research and innovation***.

Or. en

Amendment 189
Adam Bielan, Kosma Złotowski

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 a period of five years after the placing on the market ***or a shorter period, appropriate to the type and specificity of*** product with digital elements, 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 ***without undue delay take reasonable measures proportionate to the risk,*** 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 190
Marcel Kolaja
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 191
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Article 10 – paragraph 15 a (new)

Text proposed by the Commission	*Amendment*
	15 a. Manufacturers shall make publicly available communication channels such as a telephone number, electronic address or dedicated section of their website, taking into account accessibility needs for persons with disabilities, enabling users of products with digital elements to submit complaints electronically and free of charge.

Or. en

Justification

The obligation for manufacturers to include a reference to a "point of contact where information about cybersecurity vulnerabilities of the product can be reported and received" is manifestly insufficient without a proper mechanism to ensure that such reporting is acted upon. Solutions which privilege dialogue between consumers and manufacturers, such as internal or out-of-court mechanisms allow for swifter and more effective remedies for consumers.

Amendment 192
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

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 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 ***immediately*** inform the market surveillance authority about the notified vulnerability. ***Where a notified vulnerability has no corrective or mitigating measures available, ENISA shall ensure that information about the notified vulnerability is shared in line with strict security protocols and on a need-to-know-basis.***

Or. en

Amendment 193
Arba Kokalari

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***	1. The manufacturer shall, without undue delay and ***when it has a reasonable***

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.

belief that a critical or high vulnerability listed in the known exploited vulnerability catalogue referred to in paragraph 5a is present and exploitable in the product with digital elements, and after clear remediation guidance is made available, notify to ENISA ***such listed known*** 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.

Or. en

Amendment 194
Adam Bielan, Kosma Złotowski

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***	1. The manufacturer shall, notify ***relevant Computer Security Incident Response Teams (CSIRTs) or, where applicable, competent authority of the Member State established under Directive (EU) 2022/2555,*** any actively exploited vulnerability ***with significant impact on*** the product with digital elements. The notification ***shall be submitted without undue delay after the vulnerability has been addressed and*** shall include details concerning that vulnerability and, where applicable, any corrective or mitigating

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.	measures taken.

Or. en

Amendment 195
Marcel Kolaja
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, 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 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 ***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 196
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

Proposal for a regulation
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify ***to*** ENISA any incident having impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.	2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, ***by means of an early warning,*** notify ENISA ***of*** any incident having ***a significant*** impact on the security of the product with digital elements.
	The manufacturer shall without undue delay and in any event within 72 hours of becoming aware of the significant incident related to the product with digital elements further notify ENISA more details on the significant incident.
	ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and ***immediately*** inform the market surveillance authority about the notified 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

Amendment 197
Arba Kokalari

Proposal for a regulation
Article 11 – paragraph 2

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

Or. en

Amendment 198
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The manufacturer shall, without undue delay ***and in any event within 24 hours of becoming*** aware ***of it***, notify to ***ENISA any*** incident having impact on the security of the product with digital elements. ***ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents.*** The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.	2. The manufacturer shall, without undue delay ***from the moment it becomes*** aware, notify to ***relevant CSIRTs or, where applicable, competent authority of the Member State established under Directive (EU) 2022/2555, any major*** incident having ***a significant*** impact on the security of the product with digital elements. The incident notification shall ***be submitted without undue delay and*** include information ***strictly necessary to make the competent authority aware of the incident, and where relevant and proportionate to the risk,*** on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

Or. en

Amendment 199
Adam Bielan, Kosma Złotowski

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. ***CSIRTs or, where applicable, competent authority of the Member State established under Directive (EU) 2022/2555,*** shall submit to ***ENISA*** 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. ***ENISA shall submit the information***

	received by the CSIRTs or, where applicable, competent authority of the Member State established under Directive (EU) 2022/2555, to the European cyber crisis liaison organisation network (EUCyCLONe) established by Article 16 of Directive (EU) 2022/2555.

Or. en

Amendment 200
Arba Kokalari

Proposal for a regulation
Article 11 – paragraph 3

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

Or. en

Amendment 201
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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	4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and about corrective measures that the user can

the user can deploy to mitigate the impact of the incident.	deploy to mitigate the impact of the incident***, and provide them with technical information on the exploited vulnerability, concerned data and potential damage***.

Or. en

Amendment 202
Adam Bielan, Kosma Złotowski

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 ***a significant*** incident ***having major impact on the security of the product with digital elements*** and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

Or. en

Amendment 203
Arba Kokalari

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***, where appropriate and if likely to be adversely affected by the significant*** incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

Or. en

Amendment 204
Marcel Kolaja
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 205
Adam Bielan, Kosma Złotowski

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***, after consulting stakeholders and CSIRTs*** may, by means of implementing acts, specify further the type of information, format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those implementing acts shall be ***based on European and international standards, such as ISO/IEC 29147 and*** adopted in accordance with the examination procedure referred to in Article 51(2).

Or. en

Amendment 206
Arba Kokalari

Proposal for a regulation
Article 11 – paragraph 6

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

Or. en

Amendment 207
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 11 – paragraph 6

Text proposed by the Commission	*Amendment*
6. ENISA, on the basis of the notifications received pursuant to paragraphs 1 ***and 2***, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article ***[Article X]*** of Directive ***[Directive XXX/XXXX (NIS2)]***. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.	6. ENISA, on the basis of the notifications received pursuant to paragraphs 1***, 2 and 3***, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article ***14*** of Directive ***(EU) 2022/2555***. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.

Or. en

Amendment 208
Marcel Kolaja
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 209
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 11 a (new)

Text proposed by the Commission	*Amendment*
	Article 11 a
	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 210
Marcel Kolaja
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*
	(c a) all the documents proving the fulfilment of the requirements set in this article have been received from the manufacturer and are available for inspection.

Or. en

Amendment 211
Marcel Kolaja
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	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.	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 212
Marcel Kolaja
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*
	(b a) they have received from the importer all the information and documentation required by this regulation.

Or. en

Amendment 213
Marcel Kolaja
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	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.	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 214
Brando Benifei

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

Amendment 215
Marcel Kolaja
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 216
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
	1 a. The Commission shall, as provided in Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the requirements set out in Annex I.

Or. en

Amendment 217
Adam Bielan, Kosma Złotowski

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 218
Adam Bielan, Kosma Złotowski

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).	***deleted***

Or. en

Amendment 219
Adam Bielan

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

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

products with digital elements, and provided that the standard is published as a separate version by one of the European Standardisation Organisations.

Or. en

Justification

Ensuring the security of products with digital elements is of paramount importance for economic operators, market surveillance authorities, and the general public. To achieve this objective, it is essential to have available standards that elevate the level of security. Since the complete development of sectoral standards for all products within the scope of this Regulation will require a significant amount of time, it should be permissible in the initial stages of its implementation to refer to international standards in their current form.

Amendment 220
Adam Bielan, Kosma Złotowski

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).	

(This amendment applies throughout the text to all references of Common specifications.)

Or. en

Amendment 221
Arba Kokalari

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)***.	***1.*** The Commission ***may adopt implementing acts establishing common specifications covering technical*** requirements ***that provide a means*** to comply with the ***essential health and safety requirements set out in Annex I for products within the scope of this Regulation. Those implementing acts shall only be adopted*** where the ***following conditions are fulfilled:***
	(a) the Commission has ***requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more*** European standardisation organisations ***to draft a harmonised standard for*** the essential requirements set out in Annex I ***and:***
	(i) the request has not been accepted; or
	(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) 1025/2012; or

(iii) the harmonised standards do not comply with the request; and

(b) no reference to harmonised standards covering the requirements set out in Annex I has been published in the Official Journal of the European Union in accordance with Regulation (EU) 1025/2012 and no such reference is expected to be published within a reasonable period. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article ***48(3)***.

2. Before preparing the draft implementing act referred to in paragraph 3, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) 1025/2012 that it considers that the conditions in paragraph 3 have been fulfilled.

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

4. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) 1025/2012. When reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the implementing acts referred to in paragraph 1, or parts thereof which cover the same requirements as those covered by that harmonised standard.

5. When a Member State considers that a common specification does not entirely satisfy the requirements set out in Annex I, it shall inform the Commission thereof by submitting a detailed explanation. The

Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.

Or. en

Amendment 222
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

Proposal for a regulation
Article 20 – paragraph 2

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

Or. en

Amendment 223
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

Proposal for a regulation
Article 20 a (new)

Text proposed by the Commission	*Amendment*
	Article 20 a
	EU Declaration of Incorporation for partly completed products with digital elements
	1. The EU declaration of incorporation shall be drawn up by manufacturers in accordance with Article 10(7) and state

that the fulfilment of the relevant essential requirements set out in Annex I has been demonstrated.

2. The EU declaration of incorporation shall have the model structure set out in Annex IVa (new). Such a declaration shall be updated as appropriate. It shall be made available in the language or languages required by the Member State in which the partly completed product with digital elements is placed on the market or made available.

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

4. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by adding elements to the minimum content of the EU declaration of incorporation as set out in Annex IVa (new) to take account of technological developments.

Or. en

Amendment 224
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Article 22 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the	1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the

nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 20 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product.	nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 20 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product. ***In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.***

Or. en

Amendment 225
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Article 22 – paragraph 3

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

Or. en

Amendment 226
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Article 22 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall build upon	5. Member States shall build upon

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

Or. en

Amendment 227
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Article 22 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Commission may, by means of ***implementing*** acts, lay down technical specifications for pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use. Those ***implementing*** acts shall be adopted in accordance with the ***examination*** procedure referred to in Article ***51(2)***.	6. The Commission may, by means of ***delegated*** acts, lay down technical specifications for ***labelling schemes, including harmonised labels,*** pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use ***among businesses and consumers and to increase public awareness about security of products with digital elements***. Those ***delegated*** acts shall be adopted in accordance with the procedure referred to in Article ***50***.

Or. en

Amendment 228
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
	6 a. The Commission shall present easy-to-understand guidelines for businesses with the requirements of this Regulation. When developing such guidelines, the Commission should take into consideration needs of SMEs so as to keep administrative and financial burdens to a minimum while facilitating their compliance with this Regulation. The Commission should consult relevant stakeholders, with expertise in the field of cybersecurity.

Or. en

Amendment 229
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

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

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

Or. en

Amendment 230
Marcel Kolaja
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 231
Arba Kokalari

Proposal for a regulation
Article 23 – paragraph 3

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

Or. en

Amendment 232
Arba Kokalari

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	***deleted***

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.

Or. en

Amendment 233
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini

Proposal for a regulation
Article 23 – paragraph 5

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

Or. en

Amendment 234
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

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

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

Or. en

Amendment 235
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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 product with digital elements 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:

Or. en

Justification

Critical products meeting the criteria set out in Article 6 should always undergo an independent third-party assessment. Moreover, the most effective way to achieve that would be for the CRA proposal to require all 'critical products with digital elements' listed in Annex III to undergo mandatory European cybersecurity certification at the level of assurance set at "high" as established in the Cybersecurity Act (CSA). Such a certification at level "high" ensures that the product has been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. This level also guarantees that evaluators will use penetration testing, meaning that they will try to hack the device.

Amendment 236
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn

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

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

Or. en

Amendment 237
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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, 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 238
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
	4 a. For products to which Union harmonisation legislation based on the

New Legislative Framework apply, the manufacturer shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in Chapter 3 shall apply to those products.

Or. en

Amendment 239
Marcel Kolaja
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 240
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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	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.	(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, including by establishing a framework for providing appropriate financial support.***

Or. en

Amendment 241
Adam Bielan, Kosma Złotowski

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

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

Or. en

Amendment 242
Arba Kokalari

Proposal for a regulation
Article 24 a (new)

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

following conformity assessment procedures:

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

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

Or. en

Amendment 243
Marcel Kolaja
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 244
Arba Kokalari

Proposal for a regulation
Article 27 – paragraph 5

Text proposed by the Commission	*Amendment*
5. A notifying authority shall	5. A notifying authority shall

safeguard the confidentiality of the information it obtains.	safeguard the confidentiality of the information it obtains***, especially trade secrets and proprietary information***.

Or. en

Amendment 245
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
	6 a. A notifying authority shall be organised in such a way so that bureaucracy and fees are at an absolute minimum, especially for SMEs.

Or. en

Amendment 246
Arba Kokalari

Proposal for a regulation
Article 29 – paragraph 10

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

Or. en

Amendment 247
Arba Kokalari

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 SMEs in relation to fees ***and also respecting the confidentiality of trade secrets and proprietary information***.

Or. en

Amendment 248
Marcel Kolaja
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 249
Adam Bielan, Kosma Złotowski

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

Justification

Both paragraphs seem to be addressing the same issue. The link is established to avoid ambiguity.

Amendment 250
Arba Kokalari

Proposal for a regulation
Article 36 – paragraph 3

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

Or. en

Amendment 251
Arba Kokalari

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	2. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for economic operators***, with special considerations for SMEs***. Conformity

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.

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.

Or. en

Amendment 252
Adam Bielan, Kosma Złotowski

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 253
Arba Kokalari

Proposal for a regulation
Article 39 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification	The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification

policy.	policy. ***Experience and knowledge which also can facilitate corporate compliance must also be made publicly available by the Commission.***

Or. en

Amendment 254
Arba Kokalari

Proposal for a regulation
Article 40 – paragraph 1

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

Or. en

Amendment 255
Arba Kokalari

Proposal for a regulation
Article 40 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.	2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives***, in a way that reduces bureaucracy and fees***.

Or. en

Amendment 256
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

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. 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 ***effectively*** cooperate with ENISA. ***The market surveillance authorities may request ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation, including during investigations in accordance with Article 43.***

Or. en

Justification

Enforcement at national level should be reinforced on a technical level.

Amendment 257
Marcel Kolaja
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***	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.

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

Or. en

Amendment 258
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	3 a. 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 259
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Article 41 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission shall facilitate the	7. The Commission shall facilitate the

exchange of experience between designated market surveillance authorities.	***regular and structured*** exchange of experience between designated market surveillance authorities***, including via a dedicated administrative cooperation group (ADCO) established under paragraph 11 of this Article***.

Or. en

Amendment 260
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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 the Commission. ***Market surveillance authorities shall be equipped to receive complaints by consumers affected by products with digital elements if they consider that the relevant products or the practices engaged infringe this Regulation, and shall facilitate the active participation of civil society in market surveillance activities, including scientific, research and consumer organisations, by establishing a clear and accessible mechanism to facilitate reporting of vulnerabilities, incidents, and cyber threats.***

Or. en

Amendment 261
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Article 41 – paragraph 11

Text proposed by the Commission	*Amendment*
11. A dedicated administrative cooperation group (ADCO) shall be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. This ADCO shall be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of single liaison offices.	11. A dedicated administrative cooperation group (ADCO) shall be established for the uniform application of this Regulation, ***to facilitate structured cooperation in relation to the implementation of this Regulation and to streamline the practices of market surveillance authorities within the Union,*** pursuant to Article 30(2) of Regulation (EU) 2019/1020. This ADCO ***shall have, in particular, the tasks referred to in Article 32(2) of Regulation (EU) 2019/1020 and*** shall be composed of representatives of the designated market surveillance authorities***, ENISA*** and, if appropriate, representatives of single liaison offices. ***The ADCO shall meet at regular intervals and, where necessary, at the duly justified request of the Commission or ENISA or a Member State and shall coordinate its action with other existing Union activities related to market surveillance and consumer safety and, where relevant, shall cooperate and exchange information with other Union networks, groups and bodies. The ADCO may invite experts and other third parties, including consumer organisations, to attend its meetings.***

Or. en

Amendment 262
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
	11 a. For products with digital elements falling within the scope of this Regulation, distributed, put into service or used by financial institutions regulated by

relevant Union legislation on financial services, the market surveillance authority for the purposes of this Regulation shall be the relevant authority responsible for the financial supervision of those institutions under that legislation.

Or. en

Amendment 263
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	11 a. 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

Amendment 264
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 41 a (new)

Text proposed by the Commission	*Amendment*
	Article 41 a
	Expert group on technical matters
	1. The Commission shall establish an expert group in order to provide technical advice to the Commission and competent

authorities on matters related to in the implementation and enforcement of this Regulation. In particular, the expert group shall provide non-binding evaluations of products with digital elements upon request by a market surveillance authority that is conducting an investigation under Article 43 and guidance on the application of relevant concepts to software and the exclusion of free and open source software.

2. The expert group shall consist of independent experts appointed for a renewable three-year term by the Commission on the basis of their scientific or technical expertise in the field. The Commission shall appoint a number of experts which is deemed sufficient to fulfil the foreseen needs, ensuring that their professional background and affiliations result in a balanced representation of stakeholder interests, in particular open source organisations, national accreditation bodies, conformity assessment bodies pursuant to Regulation (EC) 765/2008 of the European Parliament and of the Council, data protection authorities, as well as academia and consumer organisations.

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

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

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

Or. en

Amendment 265
Arba Kokalari

Proposal for a regulation
Article 42 – paragraph 1

Text proposed by the Commission	*Amendment*
Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the respective economic operator.	Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the respective economic operator. ***Where appropriate, and in accordance with Article 52(1) point (a), this shall be in a secure, controlled environment determined by the manufacturer.***

Or. en

Amendment 266
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable	Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation ***or otherwise present threat to national security***, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the

period, commensurate with the nature of the risk, as it may prescribe.	market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

Or. en

Amendment 267
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within ***a reasonable*** period, commensurate with the nature of the risk***, as it may prescribe***.	Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant ***economic*** operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within ***an adequate*** period, commensurate with the nature of the risk.

Or. en

Amendment 268
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
Where the manufacturer of a product with digital elements does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict that product being made	Where the manufacturer of a product with digital elements does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph***, or the relevant Member States authority consider product to present threat to the national security***, the market surveillance

available on its national market, to withdraw it from that market or to recall it.

authority shall take all appropriate provisional measures to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it.

Or. en

Amendment 269
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 43 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Where, within three months of receipt of the information referred to in paragraph 4, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the operator concerned in accordance with Article 18 of Regulation (EU) 2019/1020.	7. Where, within three months of receipt of the information referred to in paragraph 4, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. ***The decision referred to in paragraph 1, concerning threat to national security shall always be deemed justified.*** This is without prejudice to the procedural rights of the operator concerned in accordance with Article 18 of Regulation (EU) 2019/1020.

Or. en

Amendment 270
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 45 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements that	1. Where the Commission has sufficient reasons to consider, including based on information provided by ***the competent authorities of Member States,***

presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it may request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.	***the computer security incident response teams (CSIRTs) designated or established in accordance with Directive (EU) 2022/2555 or*** ENISA, that a product with digital elements that presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it may request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.

Or. en

Amendment 271
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 45 – paragraph 1

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

Or. en

Amendment 272
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 45 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission ***has*** sufficient reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission may request ***ENISA*** to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. ***The relevant economic operators shall cooperate as necessary with ENISA.***	2. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission sufficient reasons***, substantiated by relevant data,*** to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission may request ***the relevant Member State authority*** to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities ***and ENISA*** accordingly.

Or. en

Amendment 273
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 45 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In ***exceptional*** circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has ***sufficient*** reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***may*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic	2. In circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***shall*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall

operators shall cooperate as necessary with ENISA.	cooperate as necessary with ENISA.

Or. en

Amendment 274
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Article 45 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In ***exceptional*** circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has ***sufficient*** reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***may*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.	2. In circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***shall*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

Or. en

Amendment 275
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 45 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Based on ***ENISA's*** evaluation, the Commission may decide that a corrective or restrictive measure is necessary at Union	3. Based on ***the Member State authority's*** evaluation ***and recommendation***, the Commission may

level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.

decide that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.

Or. en

Amendment 276
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 46 – paragraph 1

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

Or. en

Amendment 277
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 46 – paragraph 2

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

Or. en

Amendment 278
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 46 – paragraph 6

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

Or. en

Amendment 279
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 46 – paragraph 7

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

Or. en

Amendment 280
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 46 – paragraph 8

Text proposed by the Commission	*Amendment*
8. Based on ENISA's evaluation referred to in paragraph 7, the Commission ***may*** establish that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay	8. Based on ENISA's evaluation referred to in paragraph 7, the Commission ***shall*** establish that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay

consult the Member States concerned and the relevant operator or operators.	consult the Member States concerned and the relevant operator or operators.

Or. en

Amendment 281
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Article 48 – paragraph 2

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

Or. en

Amendment 282
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 48 – paragraph 2

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

Or. en

Amendment 283
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 49 – paragraph 1

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

Or. en

Amendment 284
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 49 – paragraph 2

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

Or. en

Amendment 285
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 49 – paragraph 3

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

Or. en

Amendment 286
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 49 – paragraph 4

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

Or. en

Amendment 287
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 49 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Market surveillance authorities ***may***	5. Market surveillance authorities

invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.	***shall*** invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.

Or. en

Amendment 288
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Article 49 a (new)

Text proposed by the Commission	*Amendment*
	Article 49 a
	Provision of technical advice
	1. The Commission shall appoint by way of an implementing act an expert group to provide technical advice to market surveillance authorities on matters related to the implementation and enforcement of this Regulation. The implementing act shall specify, inter alia, the details related to the composition of the group, its operation and the remuneration of its members. In particular, the expert group shall provide non-binding evaluations of products with digital elements upon request by a market surveillance authority that is conducting an investigation under Article 43 and of the list of critical products with digital elements set out in Annex II, as well as on the possible need to update that list.
	2. The expert group shall consist of independent experts appointed for a renewable three-year term by the Commission on the basis of their scientific or technical expertise in the field.
	3. The Commission shall appoint a number of experts which is deemed sufficient to fulfil the foreseen needs.

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

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

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

Or. en

Justification

Enforcement at national level should be reinforced on a technical level.

Amendment 289
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 52 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) intellectual property rights***, and confidential business information*** or trade secrets ***of a natural or legal person, including source code, except the cases referred to in Article 5 of*** Directive 2016/943 of the European Parliament and of the Council[36] ;	(a) intellectual property rights or trade secrets ***in line with*** Directive 2016/943 of the European Parliament and of the Council [36] ;
[36] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure	[36] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

(OJ L 157, 15.6.2016, p. 1).	(OJ L 157, 15.6.2016, p. 1).

Or. en

Amendment 290
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Article 53 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to ***15 000 000*** EUR or, if the offender is an undertaking, up to ***2.5*** % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.	3. The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to ***30 000 000*** EUR or, if the offender is an undertaking, up to ***6*** % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

Or. en

Justification

Article 53(3) sets maximum fines of 2,5% of the total worldwide annual turnover, a lower threshold when compared to other recent digital legislation. The proposed AI Act and the DSA set fines up to six percent of the total worldwide annual turnover. CRA should therefore be in alignment with the AIA and DSA and set maximum fines at 6% of total worldwide annual turnover.

Amendment 291
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Article 53 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to ***10***	4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to ***15***

000 000 EUR or, if the offender is an undertaking, up to ***2*** % of its total worldwide annual turnover for the preceding financial year, whichever is higher.	***000 000*** EUR or, if the offender is an undertaking, up to ***2.5*** % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Or. en

Amendment 292
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
	(a a) the type of manufactured product and whether entity qualifies as microenterprise for the specific compliance regime outlined in the Article 10(-1) of this Regulation.

Or. en

Amendment 293
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 294
Morten Løkkegaard, Andrus Ansip, Dita Charanzová, Svenja Hahn, Stéphanie Yon-Courtin, Sandro Gozi

Proposal for a regulation
Chapter VII a (new)

Text proposed by the Commission	*Amendment*
	CHAPTER VIIa
	MEASURES IN SUPPORT OF INNOVATION:
	Article 53a
	Regulatory sandboxes
	1. The Commission and ENISA, shall establish a European regulatory sandbox with voluntary participation of manufacturers of products with digital elements to:
	(a) provide for a controlled environment that facilitates the development, testing and validation of the design, development and production of products with digital elements, before their placement on the market or putting into service pursuant to a specific plan;
	(b) provide practical support to economic operators, including via guidelines and best practices to comply with the essential requirements set out in Annex I.
	(c) contribute to evidence-based regulatory learning.

Or. en

Amendment 295
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Article 54 a (new)

Text proposed by the Commission	*Amendment*
	Article 54 a
	Amendment to Directive 2020/1828/EC
	In Annex I to Directive 2020/1828/EC the following point is added:
	'67. [Regulation XXX][Cyber Resilience Act]'.

Or. en

Justification

This amendment includes this Regulation to Annex I of the Representative Actions Directive to ensure that consumers can file collective claims for breaches of these new rules.

Amendment 296
Arba Kokalari

Proposal for a regulation
Article 55 – paragraph 1

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

Or. en

Amendment 297
Carlo Fidanza

Proposal for a regulation
Article 55 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3 a. By way of derogation, for products with digital elements falling in scope of Regulation [Machinery Regulation proposal] or Regulation (EU) 167/2013 of the European Parliament and of the Council, the application date referred to Article 57 is extended by [36 months].

Or. en

Justification

For highly complex products like agricultural and construction, the necessary electronics hardware updates and machine network architecture updates are significant and need to be done per each single type/model. These industries are characterized by low volumes and many types/models.• Complex machinery will require dedicated cybersecurity standards, based on specific use cases and applications. Once they are available, manufactures will need time to re-design their products.• The machinery industry has long development cycles since the products are made for very specialized operation and have long (10+ years) lifecycles. • Updating such machinery will require multiple hardware and software design changes.• After the previous steps, the validation phase will have to start, and this takes time too. For example, agricultural machines are dependent on harvesting season for conducting field test.

Amendment 298
Carlo Fidanza

Proposal for a regulation
Article 55 – paragraph 3 b (new)

Text proposed by the Commission	*Amendment*
	3 b. By way of derogation for products with digital elements falling in scope of Regulation [Machinery Regulation proposal] or Regulation 2013/167, where the annual new sales in the EU of each type are fewer than [1000] units, the application date referred to Article 57 is extended by [60 months].

Or. en

Justification

A longer lead time should be granted to accompany small volumes productions of complex products like industrial machinery aimed at maintaining a level playing field: manufacturers will have a lot of different machine models to update and it will not be feasible to updates dozens of different models within one single cut-off date. This will be very useful to support the many SMEs still active in the agricultural machinery sector (as well as other sectors) as the one size fits for all approach might severely damage their single market competitiveness.

Amendment 299
Adam Bielan, Kosma Złotowski

Proposal for a regulation
Article 57 – paragraph 2

Text proposed by the Commission	*Amendment*
It shall apply from [***24*** months after the date of entry into force of this Regulation]. However Article 11 shall apply from [***12*** months after the date of entry into force of this Regulation].	It shall apply from [***36*** months after the date of entry into force of this Regulation]. However Article 11 shall apply from [***24*** months after the date of entry into force of this Regulation] ***and Articles 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38 shall apply from [30 months after the entry into force of this Regulation]***.

Or. en

Justification

The provisions regarding the notification of conformity assessment bodies included in Chapter IV shall be established in advanced to ensure that when all provisions of the Regulation become applicable, notified bodies are available.

Amendment 300
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 57 – paragraph 2

Text proposed by the Commission	*Amendment*
It ***shall apply from [24 months after the date of entry into force of this Regulation]. However Article 11*** shall	It shall apply from [12 months after the date of entry into force of this Regulation].

apply from [12 months after the date of entry into force of this Regulation].

Or. en

Amendment 301
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

Proposal for a regulation
Article 57 – paragraph 2

Text proposed by the Commission	*Amendment*
It ***shall apply from [24 months after the date of entry into force of this Regulation]. However Article 11*** shall apply from [12 months after the date of entry into force of this Regulation].	It shall apply from [12 months after the date of entry into force of this Regulation].

Or. en

Justification

This amendment harmonizes the date of application of the CRA, reducing it to match the 12 months already proposed for the reporting obligations on manufacturers under Article 11. Although it is understandable that manufacturers, notified bodies and Member States should have enough time to adapt to the new requirements, there can be no technical justification to further delay the application of these rules for a long period of time. This is especially clear when comparing the CRA to other similar legislation just recently adopted. For instance, both DSA and DMA, more complex digital legislations, have a shorter application period of 15 months after entry into force.

Amendment 302
Arba Kokalari

Proposal for a regulation
Article 57 – paragraph 2

Text proposed by the Commission	*Amendment*
It shall apply from [***24*** months after the date of entry into force of this Regulation]. However Article 11 shall apply from [12 months after the date of entry into force of	It shall apply from [***48*** months after the date of entry into force of this Regulation]. However Article 11 shall apply from [12 months after the date of entry into force of

this Regulation].

this Regulation].

Or. en

Amendment 303
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;	(2) Products with digital elements shall be delivered without any known ***critical or high severity*** exploitable vulnerabilities;

Or. en

Amendment 304
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
(2) Products with digital elements shall be delivered ***without any known exploitable vulnerabilities***;	(2) Products with digital elements shall be delivered ***in a way that does not wilfully create cybersecurity risks***;

Or. en

Amendment 305
Carlo Fidanza

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

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

shall:	elements shall: ***(aa) be placed on the market without any known exploitable vulnerabilities towards an external device or network;***

Or. en

Justification

Finding out exploitable vulnerabilities is possible through risk assessment, based on the ability to harm and the difficulty to exploit the vulnerability itself. Adding that all depends on a cybersecurity risk assessment is important to identify vulnerabilities and put mitigation measures in place. In line with scope clarification, it is also useful to clearly state from where the vulnerability may come.

Amendment 306
Arba Kokalari

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

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

Or. en

Amendment 307
Adam Bielan, Kosma Złotowski

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

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

Or. en

Amendment 308
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	(a a) be placed on the market with functional separation of security updates from functionality updates, to allow automatic installation of security updates, with a clear and easy-to-use opt-out mechanism, and preserve user choice on functionalities unless technically unfeasible;

Or. en

Amendment 309
Arba Kokalari

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

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

Or. en

Amendment 310
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, ***such as by*** encrypting relevant data at rest or in transit by state of the art mechanisms;	(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, encrypting relevant data at rest or in transit by state of the art mechanisms***, and by using other technical means***;

Or. en

Amendment 311
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 312
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

of service attacks;

Or. en

Amendment 313
Arba Kokalari

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

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

Or. en

Amendment 314
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 315
Arba Kokalari

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

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

Or. en

Amendment 316
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 317
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 318
Arba Kokalari

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

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

Or. en

Amendment 319
Arba Kokalari

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

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

Or. en

Amendment 320
Marcel Kolaja

on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 321
Arba Kokalari

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

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

Or. en

Amendment 322
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;	(7) provide for mechanisms to securely distribute ***security*** updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

Or. en

Amendment 323
Arba Kokalari

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

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

Or. en

Amendment 324
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
2. the point of contact where	2. the ***single*** point of contact where

information about cybersecurity vulnerabilities of the product can be reported and received;	information about cybersecurity vulnerabilities of the product can be reported and received;

Or. en

Amendment 325
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 326
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini, Brando Benifei

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

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

Or. en

Amendment 327
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini

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

Text proposed by the Commission	*Amendment*
8. the type of technical security support offered by the manufacturer and until when it will be provided***, at the very least until when users can expect to receive security updates***;	8. the type of technical security support offered by the manufacturer and until when it will be provided;

Or. en

Amendment 328
Adriana Maldonado López, Maria-Manuel Leitão-Marques, Marc Angel, Maria Grapini

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

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

Or. en

Justification

This amendment introduces the necessity to clearly and understandably specify and display, in an easily accessible manner, the end date for the expected product lifetime and, where applicable, on the packaging of the product.

Amendment 329
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
(a) the necessary measures during initial commissioning and throughout the	***deleted***

lifetime of the product to ensure its secure use;

Or. en

Amendment 330
Arba Kokalari

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

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

Or. en

Amendment 331
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 332
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
(d) the secure decommissioning of the	***deleted***

product, including information on how user data can be securely removed.

Or. en

Amendment 333
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 334
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 335
Marcel Kolaja
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
18. Routers, modems intended for the	***deleted***

connection to the internet, and switches, not covered by class II;

Or. en

Amendment 336
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 337
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 338
Marcel Kolaja
on behalf of the Verts/ALE Group

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

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

Or. en

Amendment 339
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Annex III – Part II – point 15 a (new)

Text proposed by the Commission	*Amendment*
	15 a. Smart home products, including smart home servers and virtual assistants;

Or. en

Amendment 340
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Annex III – Part II – point 15 b (new)

Text proposed by the Commission	*Amendment*
	15 b. Smart security devices, including smart door locks, cameras and alarm systems;

Or. en

Amendment 341
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Annex III – Part II – point 15 c (new)

Text proposed by the Commission	*Amendment*
	15 c. Smart toys and similar devices likely to interact with children;

Or. en

Amendment 342
Marcel Kolaja
on behalf of the Verts/ALE Group

Proposal for a regulation
Annex III – Part II – point 15 d (new)

Text proposed by the Commission	*Amendment*
	15 d. Personal health appliances and wearables.

Or. en

Amendment 343
Adam Bielan, Kosma Złotowski

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

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

Or. en

Amendment 344
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
2. a description of the design, development and production of the product and vulnerability handling processes, including:	***deleted***
(a) complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;	
(b) complete information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;	
(c) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.	

Or. en

Amendment 345
Arba Kokalari

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

Text proposed by the Commission	*Amendment*
(a) complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or	***deleted***

a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;

Or. en

Amendment 346
Arba Kokalari

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

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

Or. en

Amendment 347
Adam Bielan, Kosma Złotowski

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

Text proposed by the Commission	*Amendment*
3. ***an assessment*** of the cybersecurity risks against which the product with digital elements is designed, developed, produced,	3. ***a statement*** of the cybersecurity risks against which the product with digital elements is designed, developed, produced,

delivered and maintained as laid down in Article 10 of this Regulation;	delivered and maintained as laid down in Article 10 of this Regulation;

Or. en