



Council of the European Union
General Secretariat

Brussels, 06 October 2023

Interinstitutional files:
2022/0272 (COD)

WK 12787/2023 INIT

LIMITE

CYBER

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on cyber issues (attachés)
Subject:	Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - 4-column table - 4-column table

Delegations will find in the annex the 4-column table related to the above legislative proposal, for the HWPCI meeting on 9 October 2023.

**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on
horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU)
2019/1020 (Text with EEA relevance)**

2022/0272(COD)

[Version for Technical Meeting on 6 October, 2023]

06-10-2023 at 14h43

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Formula				
1	2022/0272 (COD)	2022/0272 (COD)	2022/0272 (COD)	2022/0272 (COD) Text Origin: Commission Proposal
Proposal Title				
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 <u>and Directive 2020/1828/EC</u> <u>(Cyber Resilience Act)</u> (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements ~~and~~ , amending Regulation (EU) 2019/1020 and Directive (EU) 2020/1828 (Text with EEA relevance)	
Formula				
3	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	EUROPEAN UNION,	EUROPEAN UNION,	EUROPEAN UNION,	EUROPEAN UNION, Text Origin: Commission Proposal
Citation 1				
4	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof, Text Origin: Commission Proposal
Citation 2				
5	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission, Text Origin: Commission Proposal
Citation 3				
6	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments, Text Origin: Commission Proposal
Citation 4				
7	Having regard to the opinion of the European Economic and Social	Having regard to the opinion of the European Economic and Social	Having regard to the opinion of the European Economic and Social	Having regard to the opinion of the European Economic and Social

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Committee ¹ , <u>1. OJ C , , p. .</u>	Committee ¹ , <u>1. [1] OJ C 100, 16.3.2023, p. 101 ~~QJ C~~</u> ~~1. p. .~~	Committee ¹ , <u>1. OJ C , , p. .</u>	Committee ¹ , <u>1. [1] OJ C 100, 16.3.2023, p. 101 ~~QJ C~~</u> ~~1. p. .~~ Text Origin: EP Mandate
Citation 5				
8	Having regard to the opinion of the Committee of the Regions ¹ , <u>1. OJ C , , p. .</u>	Having regard to the opinion of the Committee of the Regions ¹ , <u>1. OJ C , , p. .</u>	Having regard to the opinion of the Committee of the Regions ¹ , <u>1. OJ C , , p. .</u>	Having regard to the opinion of the Committee of the Regions ¹ , <u>1. OJ C , , p. .</u> Text Origin: Commission Proposal
Citation 6				
9	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure, Text Origin: Commission Proposal
Formula				
10	Whereas:	Whereas:	Whereas:	Whereas: Text Origin: Commission Proposal
Recital 1				
11	(1) It is necessary to improve the functioning of the internal market by	(1) Cybersecurity is one of the key challenges for the Union and the	(1) It is necessary to improve the functioning of the internal market by	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.	<u>number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not just on the Union's economy, but also on democracy and consumer safety and health.</u> It is <u>therefore</u> necessary to <u>strengthen the Union's approach to cybersecurity, address cyber resilience at Union level and</u> improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.	laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.	
Recital 2				
12	(2) This Regulation aims to set the boundary conditions for the	(2) This Regulation aims to set the boundary conditions for the	(2) This Regulation aims to set the boundary conditions for the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.	development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements, <u>for example by improving transparency with regard to the support period of products placed on the market.</u>	development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.	
Recital 3				
13	(3) The relevant Union legislation that is currently in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, the existing Union legislation related to cybersecurity, including [Directive XXX/XXXX (NIS2)] and Regulation (EU) 2019/881 of the European Parliament and of the Council¹ does not directly cover mandatory requirements for the security of products with digital elements. 1. Regulation (EU) 2019/881 of the European Parliament and of the Council of	(3) The relevant Union legislation that is currently in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, the existing Union legislation related to cybersecurity, including ~~fDirective XXX/XXXX (NIS2) Regulation (EU)~~ <u>and Regulation (EU) 2019/881 of the European Parliament and of the Council¹ and Directive (EU) 2022/2555</u> of the European Parliament and of the Council^{1,2} does not directly cover mandatory requirements for the security of products with digital elements.	(3) The relevant Union legislation that is currently in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, the existing Union legislation related to cybersecurity, including ~~{Directive XXX/XXXX (NIS2EU)}~~ 2022/2555 of the European Parliament and of the Council¹ and Regulation (EU) 2019/881 of the European Parliament and of the Council¹⁻² does not directly cover mandatory requirements for the security of products with digital elements.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).	1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15). <u>2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).</u>	1. ~~Regulation (EU) 2019/881~~ Directive (EU) 2022/2555 of the European Parliament and of the Council of 17 April 2019 on ENISA ~~(the European Union Agency for~~ 14 December 2022 on measures for a high common level of cybersecurity) ~~and on information and communications technology cybersecurity certification across the Union,~~ amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing ~~Regulation (EU) No 526/2013 (Cybersecurity Act)~~ Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 151, 7.6.2019, p. 15333, 27.12.2022, p. 80). 2. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).	
Recital 4				
14	(4) While the existing Union legislation applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal	(4) While the existing Union legislation applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal	(4) While the existing Union legislation applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on companies to comply with a number of requirements for similar types of products. The cybersecurity of these products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level. The Union regulatory landscape should be harmonised by introducing cybersecurity requirements for products with digital elements. In addition, certainty for operators and users should be ensured across the Union, as well as a better harmonisation of the single market, creating more viable conditions for operators aiming at entering the Union market.	market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on ~~companies~~ <u>undertakings and organisations</u> to comply with a number of requirements for similar types of products. The cybersecurity of these products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level, <u>to ensure a harmonised and clear regulatory framework for undertakings, particularly micro, small and medium-sized enterprises</u>. The Union regulatory landscape should be harmonised by introducing cybersecurity requirements for products with digital elements. In addition, certainty for operators and users should be ensured across the Union, as well as a better harmonisation of the single market <u>and proportionality for microenterprises and small and medium-sized enterprises</u>, creating more viable conditions for <u>economic</u> operators aiming at entering the Union market.	market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on companies to comply with a number of requirements for similar types of products. The cybersecurity of these products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level. The Union regulatory landscape should be harmonised by introducing cybersecurity requirements for products with digital elements. In addition, certainty for economic operators and users should be ensured across the Union, as well as a better harmonisation of the single market, creating more viable conditions for economic operators aiming at entering the Union market.	

Commission Proposal		EP Mandate	Council Mandate	Draft Agreement	
Recital 4a					
14a		<u>(4a) The horizontal nature of this Regulation means that it will have an impact on very different segments of the Union's economy. It is therefore important that the specificities of each sector are taken into account and that the cybersecurity requirements laid down in this Regulation are proportional to the risks. The Commission should therefore issue guidelines which explain in a clear and detailed manner how to apply this Regulation. Guidelines should cover inter alia a detailed explanation of the scope, in particular the notion of remote data processing and the implications for free and open-source developers, the criteria used to determine how critical products with digital elements are classified and the interplay between this Regulation and other Union law.</u>	PUBLIC		
Recital 4b					
14b		<u>(4b) A business operating online may offer a variety of different services. Depending on the nature of services provided, the same entity may fall under several different categories of economic operators. Where an entity provides online</u>			

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>intermediation services for a product with digital elements and is a provider of an online marketplace, as defined in Article 3(14) of Regulation 2023/988 of the European Parliament and of the Council¹, it does not qualify as an economic operator as defined in this Regulation. Where the same entity is a provider of an online marketplace and acts as an economic operator as defined in this Regulation, for the sale of products with digital elements, it should be subject to the scope of this Regulation with regard to such products. The provisions of Regulation (EU) 2023/988 is fully applicable to this Regulation. Given the prominent role that online marketplaces have in enabling electronic commerce, they should strive to cooperate with the market surveillance authorities of the Member States in order to ensure that products purchased through online marketplaces comply with the cybersecurity requirements laid down in this Regulation.</u> <u>1. Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).</u>		
Recital 5				
15	(5) At Union level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade¹, the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021,² have called for specific Union cybersecurity requirements for digital or connected products, with several countries around the world introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe,³ citizens called for "a stronger role for the EU in countering cybersecurity threats". 1. JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. 2. 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html. 3. Conference on the Future of Europe – Report on the Final Outcome, May 2022, Proposal 28(2). The Conference was held Between April 2021 and May 2022. It was a unique, citizen-led exercise of deliberative democracy at the pan-European level, involving thousands of European citizens as	(5) At Union level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade¹, the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021,² have called for specific Union cybersecurity requirements for digital or connected products, with several countries around the world introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe,³ citizens called for "a stronger role for the EU in countering cybersecurity threats". <u>In order for the Union to play a leading international role in the field of cybersecurity, it is important to establish an ambitious overarching regulatory framework.</u> 1. JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. 2. 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html. 3. Conference on the Future of Europe –	(5) At Union level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade¹, the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021,² have called for specific Union cybersecurity requirements for digital or connected products, with several countries around the world introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe,³ citizens called for "a stronger role for the EU in countering cybersecurity threats". 1. JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. 2. 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html. 3. Conference on the Future of Europe – Report on the Final Outcome, May 2022, Proposal 28(2). The Conference was held Between April 2021 and May 2022. It was a unique, citizen-led exercise of deliberative democracy at the pan-European level, involving thousands of European citizens as	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	well as political actors, social partners, civil society representatives and key stakeholders.	Report on the Final Outcome, May 2022, Proposal 28(2). The Conference was held Between April 2021 and May 2022. It was a unique, citizen-led exercise of deliberative democracy at the pan-European level, involving thousands of European citizens as well as political actors, social partners, civil society representatives and key stakeholders.	well as political actors, social partners, civil society representatives and key stakeholders.	

Recital 6

16	(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally.	(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally.	(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally.	(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally. Text Origin: Commission Proposal

Recital 7

17	(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.	(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.	(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.	(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.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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.	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.	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. Text Origin: Commission Proposal
Recital 8				
18	(8) By setting cybersecurity requirements for placing on the market products with digital elements, the cybersecurity of these products for consumers and for businesses alike will be enhanced. This also includes requirements for	(8) By setting cybersecurity requirements for placing on the market products with digital elements, the cybersecurity of these products for consumers and for businesses alike will be enhanced. This also includes requirements for	(8) By setting cybersecurity requirements for placing on the market products with digital elements, the cybersecurity of these products for consumers and for businesses alike will be enhanced. This also includes requirements for	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitors.	placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitors. <u>Those requirements will also ensure that cybersecurity is taken into account throughout supply chains, making final products with digital elements more secure. This will, in turn, represent a competitive advantage for manufacturers established or represented in the Union, which will be able to advertise the cybersecurity of their products.</u>	placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitors. Similarly the products with digital elements listed in Annex III and Annex IIIa to this Regulation are also relevant for consumer products. The stricter conformity assessment procedure that these products are required to comply with will contribute to prevent negative impacts of the exploitation of potential cybersecurity vulnerabilities on consumers. For instance, products with digital elements listed in Annex III and Annex IIIa, such as microprocessors, microcontrollers and general purpose operating systems, will typically be components that play an essential role for the cybersecurity of consumer products, including smart home products with safety functionalities, such as door locks and alarm systems, connected products for children, including toys and baby monitors, and wearable technology and other connected health devices.	
Recital 9				
19	(9) This Regulation ensures a high level of cybersecurity of products	(9) This Regulation ensures a high level of cybersecurity of products	(9) This Regulation ensures a high level of cybersecurity of products	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	with digital elements. ~~It does not regulate services, such as Software-as-a-Service (SaaS), except for~~ <u>and their integrated remote data processing solutions.</u> Such remote data processing solutions relating to a product with digital elements ~~understood~~ <u>are defined</u> as any data processing at a distance for which the software is designed and developed by <u>or on behalf of</u> 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)}~~ <u>For example, cloud enabled functionalities provided by the manufacturer of smart home devices that enable users to control the device at a distance, should fall within the scope of this Regulation. On the other hand, websites not inextricably linked to a product with digital elements or cloud services outside the responsibility of the manufacturer should not be considered to be remote data processing solutions under this Regulation. Directive (EU) 2022/2555</u> puts in place cybersecurity and incident reporting requirements for essential and important entities, such as critical infrastructure, with a view to	~~with digital elements. It does not regulate services, such as Software-as-a-Service (SaaS), except for~~ applies to remote data processing solutions relating to a product with digital elements ~~understood,~~ defined as any data processing at a distance for which the software or hardware is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions. ~~{Directive XXX/XXXX (NIS2)}~~ Software-as-a-Service (SaaS) solutions constitute remote data processing solutions within the meaning of this Regulation only if they meet that definition. For example, websites that do not support the functionality of a product with digital elements, or cloud services designed and developed outside the responsibility of a manufacturer of a product with digital elements are not in the scope of this Regulation. Directive (EU) 2022/2555 puts in place cybersecurity and incident reporting requirements for essential and important entities, such as critical infrastructure, with a view to increasing the resilience of the services they provide. ~~{Directive XXX/XXXX (NIS2)}~~ EU) 2022/2555	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		increasing the resilience of the services they provide. ~~fWhile Directive XXX/XXXX (NIS2EU) f~~ <u>2022/2555</u> applies to cloud computing services and cloud service models, <u>and this Regulation does not apply to services, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS), they may fall within the scope of this Regulation to the extent they meet the definition of remote data processing solutions</u> ~~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.~~	applies to cloud computing services and cloud service models, such as SaaS. All entities providing cloud computing services in the Union which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC¹, that meet or exceed the threshold ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall in the scope of that Directive. ¹ Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	
Recital 9a				
19a			(9a) The definition of products with digital elements also includes remote data processing solutions to ensure that such products are adequately secured in their entirety by their manufacturers, irrespective of whether data is processed or stored locally on the user's device or remotely by the manufacturer. The processing or storage at a distance is covered only in so far as necessary for a product with digital elements to perform its functions. This could	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			for instance be the case where a hardware device requires access to an application programming interface or a database developed by the manufacturer. For example, many smart home devices are designed to communicate with a cloud service provided by the manufacturer, which enables users to control and monitor the devices at a distance using a mobile application. In such case, the cloud service is therefore in the scope of this Regulation as a remote data processing solution. The requirements concerning the remote data processing solutions under the scope of this Regulation do not therefore entail technical, operational and organisational measures aimed at managing the risks posed to the security of their network and information systems as a whole.	
Recital 9b				
19b			(9b) In line with the objective of this Regulation to remove obstacles to the free movement of products with digital elements, Member States should not impede, for the matters covered by this Regulation, the making available on the market of products with digital elements which comply	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			with this Regulation. Therefore, for matters harmonised by this Regulation, Member States cannot impose further cybersecurity requirements for the making available on the market of products with digital elements. Any entity can however establish additional requirements to those laid down by this Regulation for the procurement or use of those products for their specific purposes and can therefore choose to use products with digital elements that meet stricter or more specific cybersecurity requirements than those applicable for the making available on the market under this Regulation. Furthermore, Directive (EU) 2022/2555 sets out cybersecurity risk-management measures for essential and important entities that could entail supply chain security measures that require the use of products with digital elements meeting stricter cybersecurity requirements than those laid down by this Regulation. In line with Directive (EU) 2022/2555 and its minimum harmonisation principle, Member States may therefore impose additional or stricter cybersecurity requirements for the use of ICT products by essential or important	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			entities under the scope of that Directive in order to ensure a higher level of cybersecurity, provided that such requirements are consistent with Member States' obligations laid down in Union law. Matters not covered by this Regulation can include non-technical factors relating to products with digital elements and the manufacturers thereof. Member States may therefore lay down national measures, including restrictions on products with digital elements or suppliers of such products, that take account of non-technical factors. National measures relating to such factors must comply with Union law.	
Recital 9c				
19c			(9c) This Regulation should be without prejudice to the Member States' prerogatives to take measures safeguarding national security, in compliance with Union law. Member States should be able to subject products with digital elements that will be used for military, defence or national security purposes, to additional measures.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 9a				
19d		<u>(9a) Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. Research by the European Commission¹ also shows that free and open-source software can contribute between EUR 65 billion to EUR 95 billion to the Union's GDP and that it can provide significant growth opportunities for the Union's 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, in particular by microenterprises and small, medium-sized enterprises, including start-ups, and not-for-profit organisations, academic research and individuals, this Regulation should apply to free and open-source software products in specific cases, to take into account the fact that different development models of software distributed and developed under public licences exist.</u> <u>1. The impact of open source software and</u>	PUBLIC	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		hardware on technological independence, competitiveness and innovation in the EU economy', European Commission, 6 September 2021 https://ec.europa.eu/newsroom/dae/redirecton/document/79021		
Recital 10				
20	(10) In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.	(10) ~~In order not to hamper innovation or research, Only~~ free and open-source software ~~developed or supplied outside~~ <u>made available on the market in</u> 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, Whether a free and open-source product has been made available as part of~~ a commercial activity ~~might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software~~ <u>should be assessed on a</u>	(10) ~~In order not to hamper innovation or research, free and open-source software developed or~~ This Regulation applies only to products with digital elements made available on the market, hence supplied outside for distribution or use on the Union market in the course of a commercial activity. The supply in the course of a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise, by providing a software platform through which the manufacturer monetises other services, or by requiring as a condition for use, the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the ~~should not be covered by this Regulation. This~~	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>product-by-product basis, looking at both the development model and the supply phase of the free and open-source product with digital elements.</u>	is in particular the case for software. The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity. Free and open-source software is understood as free software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable modified versions and redistributable, and which includes its source code and modified versions. Free and open-source software is developed, maintained, and distributed openly, including via online platforms. A package manager, code host or collaboration platform that facilitates the development and supply. In the context of software, is only considered to be a distributor if they make this software available on the market and hence supply it for distribution or use on the Union market in the course of a commercial activity. Taking account of the above-mentioned elements determining the commercial nature of an activity, this Regulation should only apply to free and open-source software that is supplied in the course of a commercial activity. Products	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			provided as part of the delivery of a service for which a fee is charged solely to recover the actual costs directly related to the operation of that service such as may be the case with certain products provided by public administration entities, should not be considered on those grounds alone a commercial activity for the purposes of this Regulation. Furthermore, products with digital elements which are developed or modified by a public administration entity 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 its own use should not be considered as made available on the market as defined by this Regulation.	
Recital 10a				
20a		<u>(10a) For example, a fully decentralised development model, where no single commercial entity exercises control over what is</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>accepted into the project's code base, should be taken as an indication that the product has been developed in a non-commercial setting. On the other hand, where free and open-source software is developed by a single organisation or an asymmetric community, where a single organisation is generating revenues from related use in business relationships, this should be considered to be a commercial activity. Similarly, where the main contributors to free and open-source projects are developers employed by commercial entities and when such developers or the employer can exercise control as to which modifications are accepted in the code base, the project should generally be considered to be of a commercial nature.</u>		
Recital 10b				
20b		<u>(10b) With regard to the supply phase, in the context of free and open-source 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 for the recuperation of actual costs, by providing a software platform</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>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. Accepting donations without the intention of making a profit should not be considered to be a commercial activity, unless such donations are made by commercial entities and are recurring in nature.</u>		
Recital 10c				
20c		<u>(10c) Developers contributing individually to free and open-source projects should not be subject to obligations pursuant to this Regulation.</u>		
Recital 10d				
20d		<u>(10d) The sole act of hosting free and open-source software on open repositories does not in itself constitute making available on the market of a product with digital elements. As such, most package managers, code hosting and collaboration platforms should not be considered to be distributors within the meaning of this Regulation.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 10e				
20e		<u>(10e) In order to ensure that the products are designed, developed and produced in accordance with the essential requirements provided for in Annex I, Section I, manufacturers should exercise due diligence when integrating components sourced from third parties, including in the case of free and open-source software that has not been made available on the market. The appropriate level of due diligence depends on the nature and the level of risk of the component and may include one or more of the following actions: checking if the component already carries the CE mark, checking security up-dates history, verifying if it is free from vulnerabilities registered in the European vulnerability database or other public databases, or carrying out additional security tests. Where, in the exercise of due diligence, the manufacturer of the product identifies a vulnerability in a component, including in a free and open-source component, it should inform the developer of the component, address and remedy the vulnerability, and, where applicable, provide the developer</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>with the applied security fix. Once the manufacturer has placed the product on the market, it should be responsible for ensuring that vulnerabilities are handled throughout the support period, including for free and open-source components integrated into the product with digital elements.</u>	PUBLIC	
Recital 10f				
20f		<u>(10f) The lack of professional skills in the field of cybersecurity is a key issue to be tackled for the successful application of this Regulation. Particular emphasis should be put on the skills gap for manufacturers, market surveillance authorities and notified bodies. Therefore, in line with the Commission's Communication entitled "Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy')", specific measures both at Union and Member States level should be put in place to assess the state and the evolution of the cybersecurity labour market and synergies for cybersecurity education and training offers also addressing the gender gap in the sector, with the aim of establishing a common Union approach to</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>cybersecurity training.</u>		
Recital 11				
21	(11) A secure Internet is indispensable for the functioning of critical infrastructures and for society as a whole. [Directive XXX/XXXX (NIS2)] aims at ensuring a high level of cybersecurity of services provided by essential and important entities, including digital infrastructure providers that support core functions of the open Internet, ensure Internet access and Internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the Internet are developed in a secure manner and that they comply with well-established Internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under the [Directive XXX/XXXX (NIS2)] by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products.	(11) A secure Internet is indispensable for the functioning of critical infrastructures and for society as a whole. ~~{Directive XXX/XXXX (NIS2 EU)}~~ <u>2022/2555</u> aims at ensuring a high level of cybersecurity of services provided by essential and important entities, including digital infrastructure providers that support core functions of the open Internet, ensure Internet access and Internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the Internet are developed in a secure manner and that they comply with well-established Internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under the ~~{Directive XXX/XXXX (NIS2 EU)}~~ <u>2022/2555</u> by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such	(11) A secure Internet is indispensable for the functioning of critical infrastructures and for society as a whole. ~~{Directive XXX/XXXX (NIS2 EU)}~~ <u>2022/2555</u> aims at ensuring a high level of cybersecurity of services provided by essential and important entities, including digital infrastructure providers that support core functions of the open Internet, ensure Internet access and Internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the Internet are developed in a secure manner and that they comply with well-established Internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under ~~the~~ ~~{Directive XXX/XXXX (NIS2 EU)}~~ <u>2022/2555</u> by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to	(11) A secure Internet is indispensable for the functioning of critical infrastructures and for society as a whole. ~~{Directive XXX/XXXX (NIS2 EU)}~~ <u>2022/2555</u> aims at ensuring a high level of cybersecurity of services provided by essential and important entities, including digital infrastructure providers that support core functions of the open Internet, ensure Internet access and Internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the Internet are developed in a secure manner and that they comply with well-established Internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under ~~the~~ ~~{Directive XXX/XXXX (NIS2 EU)}~~ <u>2022/2555</u> by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		products.	timely security updates for such products.	products. Text Origin: Council Mandate
Recital 11a				
21a			(11a) One of the most important measures for users to take in order to protect their products with digital elements from cyberattacks is to install the latest available security updates as soon as possible. Manufacturers should therefore design their products and create processes to ensure that products with digital elements include functions that enable the notification, distribution, download and installation of security updates automatically. They should also provide the possibility to approve the download and installation of the security updates as a final step, as well as clear instructions on how users can opt out of automatic updates. The requirements relating to automatic updates laid down in Annex I of this Regulation are not applicable to products primarily intended to be integrated as components into other products. They also do not apply to products with digital elements for which users would not reasonably expect automatic	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			updates, including products with digital elements intended to be used in professional ICT-networks, and especially in critical and industrial environments where an automatic update could cause interference with operations. Irrespective of whether a product with digital elements is designed to receive automatic updates or not, its manufacturer should inform users about vulnerabilities and make security updates available without delay.	
Recital 12				
22	(12) Regulation (EU) 2017/745 of the European Parliament and of the Council ¹ lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council ² lays down rules on in vitro diagnostic medical devices. Both Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole life cycle approach are also	(12) Regulation (EU) 2017/745 of the European Parliament and of the Council ¹ lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council ² lays down rules on in vitro diagnostic medical devices. Both Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole life cycle approach are also	(12) Regulation (EU) 2017/745 of the European Parliament and of the Council ¹ lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council ² lays down rules on ~~in vitro~~ diagnostic medical devices. Both Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole life cycle	(12) Regulation (EU) 2017/745 of the European Parliament and of the Council ¹ lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council ² lays down rules on <u>in vitro</u> ~~in vitro~~ diagnostic medical devices. Both Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole life cycle

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	covered by those Regulations. These requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including in vitro diagnostic devices, with guidance on how to fulfil all the relevant essential requirements of Annex I to those Regulations with regard to cybersecurity.³ Products with digital elements to which either of those Regulations apply should therefore not be subject to this Regulation. 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1). 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176). 3. MDCG 2019-16, endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745.	covered by those Regulations. These requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including in vitro diagnostic devices, with guidance on how to fulfil all the relevant essential requirements of Annex I to those Regulations with regard to cybersecurity.³ Products with digital elements to which either of those Regulations apply should therefore not be subject to this Regulation. 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1). 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176). 3. MDCG 2019-16, endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745.	approach are also covered by those Regulations. These requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including ~~in vitro~~ ~~in vitro~~ diagnostic devices, with guidance on how to fulfil all the relevant essential requirements of Annex I to those Regulations with regard to cybersecurity.³ Products with digital elements to which either of those Regulations apply should therefore not be subject to this Regulation. 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1). 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176). 3. MDCG 2019-16, endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation	approach are also covered by those Regulations. These requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including ~~in vitro~~ ~~in vitro~~ diagnostic devices, with guidance on how to fulfil all the relevant essential requirements of Annex I to those Regulations with regard to cybersecurity.³ Products with digital elements to which either of those Regulations apply should therefore not be subject to this Regulation. 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1). 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176). 3. MDCG 2019-16, endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			(EU) 2017/745.	(EU) 2017/745. Text Origin: Council Mandate
Recital 12a				
22a		<u>(12a) Products with digital elements that are developed exclusively for national security or military purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation. However, Member States are encouraged to ensure the same or higher level of protection for those products as for those falling within the scope of this Regulation.</u>		
Recital 13				
23	(13) Regulation (EU) 2019/2144 of the European Parliament and of the Council ¹ establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire lifecycle of vehicles, equipment and services in	(13) Regulation (EU) 2019/2144 of the European Parliament and of the Council ¹ establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire lifecycle of vehicles, equipment and services in	(13) Regulation (EU) 2019/2144 of the European Parliament and of the Council ¹ establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire lifecycle of vehicles, equipment and services in	(13) Regulation (EU) 2019/2144 of the European Parliament and of the Council ¹ establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire ~~lifecycle~~ <u>life cycle</u> of vehicles, equipment and services in

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	compliance with the applicable United Nations regulations on technical specifications and cybersecurity², and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council³ is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats. Products with digital elements to which Regulation (EU) 2019/2144 applies and those products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation., The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation. 1. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and	compliance with the applicable United Nations regulations on technical specifications and cybersecurity², and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council³ is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats. Products with digital elements to which Regulation (EU) 2019/2144 applies and those products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation. The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation. 1. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and	compliance with the applicable United Nations regulations on technical specifications and cybersecurity², and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council³ is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats. Products with digital elements to which Regulation (EU) 2019/2144 applies and those products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation., The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation. 1. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and	compliance with the applicable United Nations regulations on technical specifications and cybersecurity², and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council³ is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats. Products with digital elements to which Regulation (EU) 2019/2144 applies and those products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation., The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation. 1. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1). 2. UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management system [2021/387]. 3. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).	the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1). 2. UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management system [2021/387]. 3. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).	the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1). 2. UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management system [2021/387]. 3. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).	the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1). 2. UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management system [2021/387]. 3. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1). Text Origin: Council Mandate
Recital 14				
24	(14) This Regulation lays down horizontal cybersecurity rules which	(14) This Regulation lays down horizontal cybersecurity rules which	(14) This Regulation lays down horizontal cybersecurity rules which	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	are not specific to sectors or certain products with digital elements. Nevertheless, sectoral or product-specific Union rules could be introduced, laying down requirements that address all or some of the risks covered by the essential requirements laid down by this Regulation. In such cases, the application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I of this Regulation may be limited or excluded where such limitation or exclusion is consistent with the overall regulatory framework applying to those products and where the sectoral rules achieve the same level of protection as the one provided for by this Regulation. The Commission is empowered to adopt delegated acts to amend this Regulation by identifying such products and rules. For existing Union legislation where such limitations or exclusions should apply, this Regulation contains specific provisions to clarify its relation with that Union legislation.	are not specific to sectors or certain products with digital elements. Nevertheless, sectoral or product-specific Union rules could be introduced, laying down requirements that address all or some of the risks covered by the essential requirements laid down by this Regulation. In such cases, the application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I of this Regulation may be limited or excluded where such limitation or exclusion is consistent with the overall regulatory framework applying to those products and where the sectoral rules achieve the same level of protection as the one provided for by this Regulation. The Commission is empowered to adopt delegated acts to amend this Regulation by identifying such products and rules. For existing Union legislation where such limitations or exclusions should apply, this Regulation contains specific provisions to clarify its relation with that Union legislation.	are not specific to sectors or certain products with digital elements. Nevertheless, sectoral or product-specific Union rules could be introduced, laying down requirements that address all or some of the risks covered by the essential requirements laid down by this Regulation. In such cases, the application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I of this Regulation may be limited or excluded where such limitation or exclusion is consistent with the overall regulatory framework applying to those products and where the sectoral rules achieve at least the same level of protection as the one provided for by this Regulation. ~~The Commission is empowered to adopt delegated acts to amend this Regulation by identifying such products and rules.~~ For existing Union legislation where such limitations or exclusions should apply, this Regulation contains specific provisions to clarify its relation with that Union legislation.	
Recital 14a				
24a		<u>(14a) In order to ensure that</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>products made available on the market can be repaired effectively and their durability extended, an exemption should be provided for spare parts. This should be the case both for spare parts that have the purpose of repairing legacy products made available before the date of application of this Regulation as well as for spare parts that have already undergone a conformity assessment procedure pursuant to this Regulation and that are supplied by the same manufacturer.</u>		
Recital 14b				
24b		<u>(14b) Regulation (EU) 2022/2554 of the European Parliament and of the Council¹ establishes a number of requirements to ensure the security of network and information systems supporting the business processes of financial entities. The Commission should monitor the implementation of this Regulation in the financial sector, to ensure compatability and to avoid overlaps for products with digital elements that may also be covered by Regulation (EU) 2022/2554.</u> <u>1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<i>resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).</i>		
Recital 14c				
24c		<i>(14c) Agricultural and forestry vehicles that fall within the scope of Regulation (EU) 167/2013 of the European Parliament and of the Council¹ also fall within the scope of this Regulation. Future amendments to Regulation (EU) 167/2013 should avoid regulatory overlaps.</i> <i>1. Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1).</i>		
Recital 15				
25	(15) Delegated Regulation (EU) 2022/30 specifies that the essential requirements set out in Article 3(3), point (d) (network harm and misuse of network resources), point (e) (personal data and privacy) and point (f) (fraud) of Directive 2014/53/EU apply to certain radio equipment. [Commission implementation decision XXX/2022 on a standardisation request to the	(15) Commission Delegated Regulation (EU) 2022/30 ¹ specifies that the essential requirements set out in Article 3(3), point (d) (network harm and misuse of network resources), point (e) (personal data and privacy) and point (f) (fraud) of Directive 2014/53/EU apply to certain radio equipment. [Commission implementation decision XXX/2022	(15) Delegated Regulation (EU) 2022/30 specifies that the essential requirements set out in Article 3(3), point (d) (network harm and misuse of network resources), point (e) (personal data and privacy) and point (f) (fraud) of Directive 2014/53/EU apply to certain radio equipment. [Commission implementation decision XXX/2022 on a standardisation request to the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	European Standardisation Organisations] lays down requirements for the development of specific standards further specifying how these three essential requirements should be addressed. The essential requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU. Further, the essential requirements laid down in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, if the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation.	on a standardisation request to the European Standardisation Organisations] lays down requirements for the development of specific standards further specifying how these three essential requirements should be addressed. The essential requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU. Further, the essential requirements laid down in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, ~~if~~<u>when</u> the Commission ~~repeals or~~ amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation. <u>Where manufacturers comply with this Regulation before</u>	European Standardisation Organisations] lays down requirements for the development of specific standards further specifying how these three essential requirements should be addressed. The essential requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU. Further, the essential requirements laid down in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, if the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>its date of application, they should be considered also to comply with Commission Delegated Regulation (EU) 2022/30, until the Commission repeals that Delegated Regulation.</u> <u>1. Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (OJ L 7, 12.1.2022, p. 6).</u>	PUBLIC	
Recital 16				
26	(16) Directive 85/374/EEC¹ is complementary to this Regulation. That Directive sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault ('strict liability'). Where such a lack of safety consists in a lack of security updates after placing the product on the market, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such security updates	(16) <u>Council</u> Directive 85/374/EEC¹ is complementary to this Regulation. That Directive sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault ('strict liability'). Where such a lack of safety consists in a lack of security updates after placing the product on the market, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such	(16) Directive 85/374/EEC¹ is complementary to this Regulation. That Directive sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault ('strict liability'). Where such a lack of safety consists in a lack of security updates after placing the product on the market, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such security updates	(16) <u>Council</u> Directive 85/374/EEC¹ is complementary to this Regulation. That Directive sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault ('strict liability'). Where such a lack of safety consists in a lack of security updates after placing the product on the market, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	should be laid down in this Regulation. 1. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.85).	security updates should be laid down in this Regulation. 1. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, ~~7.8.85~~7.8.1985, p. 29).	should be laid down in this Regulation. 1. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.85).	security updates should be laid down in this Regulation. 1. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, ~~7.8.85~~7.8.1985, p. 29). Text Origin: EP Mandate

Recital 17

27	(17) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council¹, including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal	(17) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council¹, including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal	(17) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council¹, including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal	(17) This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council¹, including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board (EDPB) established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and the Union data protection law should also be created in the area of market surveillance and enforcement. To this end, national market surveillance authorities appointed under this Regulation should cooperate with authorities supervising Union data protection law. The latter should also have access to information relevant for accomplishing their tasks. 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1).	data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board (EDPB) established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and the Union data protection law should also be created in the area of market surveillance and enforcement. To this end, national market surveillance authorities appointed under this Regulation should cooperate with authorities supervising Union data protection law. The latter should also have access to information relevant for accomplishing their tasks. 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1).	data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board (EDPB) established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and the Union data protection law should also be created in the area of market surveillance and enforcement. To this end, national market surveillance authorities appointed under this Regulation should cooperate with authorities supervising Union data protection law. The latter should also have access to information relevant for accomplishing their tasks. 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1).	data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board (EDPB) established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and the Union data protection law should also be created in the area of market surveillance and enforcement. To this end, national market surveillance authorities appointed under this Regulation should cooperate with authorities supervising Union data protection law. The latter should also have access to information relevant for accomplishing their tasks. 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1). Text Origin: Commission Proposal

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

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	covers those requirements.	covers those requirements.	conformity for this Regulation, in so far as the certificate, or parts thereof, covers those requirements.	
Recital 18a				
28a			(18a) When integrating components sourced from third parties in products with digital elements during the design and development phase, manufacturers should exercise due diligence. The appropriate level of due diligence measures should be informed by the nature and level of the cybersecurity risk associated with the component and, for this purpose, take into account specific factors, such as the way in which the component contributes to the functionality of the product and the extent to which it has access to data processed by the product with digital elements. Depending on the risk, due diligence measures could include verifying that the manufacturer of a component has demonstrated conformity with this Regulation, verifying that a component is free from vulnerabilities registered in publicly accessible vulnerability databases, or verifying that a component receives regular security updates. The vulnerability	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			handling obligations in this Regulation, which the manufacturers have to comply with when placing a product with digital elements on the market and for the expected product lifetime, apply to products with digital elements in their entirety, including to all integrated components.	
Recital 18a				
28b		<u>(18a) When procuring products with digital elements, Member States should give priority to products that have a high level of cybersecurity and an appropriate support period, in order to improve their ability to deal with cyber threats, as well as to ensure the efficient use of public resources. Furthermore, Member States should ensure that manufacturers remedy vulnerabilities that affect publicly procured products with digital elements as soon as possible and as a matter of urgency where such products have a significant risk profile.</u>		
Recital 19				
29	(19) Certain tasks provided for in this Regulation should be carried out	(19) Certain tasks provided for in this Regulation should be carried out	(19) ~~Certain tasks provided for in this Regulation should be carried out~~	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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-	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 <u>significant</u> 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,~~ <u>#Vulnerabilities subject to mandatory reporting concern instances where an actor is executing malicious code on a</u>	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 established under ~~referred to in Directive [Directive XXX / XXXX (NIS2)]~~ 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	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	<u>product with digital elements in order to generate a security breach, for example by exploiting weaknesses in identification and authentication functions. Vulnerabilities that are discovered with no malicious intent for purposes of good faith testing, investigation, correction or disclosure to promote the security or safety of the system owner and its users</u> should <u>not be subject to mandatory notifications. A significant incident that has an impact on the security of the product</u> ~~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~~ <u>concerns a cybersecurity incident that can severely affect the development, production and maintenance processes</u> of the ~~Commission, ENISA should be able to conduct evaluations in respect of specific~~ <u>manufacturer and that in turn can significantly impact the security of its</u> products. <u>Such as significant incident could include a</u>	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~~ provide an analysis to support an evaluation 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.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>situation in which, an attacker has successfully compromised the release channel via which the manufacturer releases security updates to users</u> ~~with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.~~		
Recital 19a				
29a			(19a) Actively exploited vulnerabilities concern instances where a manufacturer establishes that an attempted or successful security breach affecting its users or any other natural or legal persons has resulted from a malicious actor making use of a flaw in one of the products with digital elements placed on the market by the manufacturer. An example of such a vulnerability could be the insufficient protection of a product against brute force attacks. Risks of reporting unpatched vulnerabilities should be minimized by technical measures and procedural agreements. Incidents having an impact on the security of the product with digital elements, on the other hand, refer to situations where a cybersecurity incident	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			affects the development, production or maintenance processes of the manufacturer in such a way that it could result in an increased cybersecurity risk for users or other persons. An example of such incident is a security breach on the manufacturer's network allowing unauthorised persons to introduce malicious code into a product in development or into a release channel that provides users with automatic updates.	
Recital 19a				
29b		<i><u>(19a) 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 (EU) 2022/2555, and inform the relevant market surveillance authorities about the notified vulnerability. ENISA should ensure that those notifications are received, stored and transmitted via secure channels and that clear protocols are in place with regard to who can access them and the arrangements for their onward transmission. ENISA should ensure</u></i>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>the confidentiality of those notifications with particular regard to vulnerabilities for which a security update is not yet available. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive (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. 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</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>market.</u>		
Recital 20				
30	(20) Products with digital elements should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.	(20) Products with digital elements should bear the CE marking to <u>visibly, legibly and indelibly</u> indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking. <u>Furthermore, at trade fairs, exhibitions and demonstrations or similar events, Member States should not prevent the presentation and use of a prototype product with digital elements.</u>	(20) Products with digital elements should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.	
Recital 21				
31	(21) In order to ensure that manufacturers can release software for testing purposes before subjecting their products to conformity assessment, Member States should not prevent the making available of unfinished software, such as alpha versions, beta versions or release candidates, as long as the version is only made available for	(21) In order to ensure that manufacturers can release software for testing purposes before subjecting their products to conformity assessment, Member States should not prevent the making available <u>in a non-production version</u> of unfinished software, such as alpha versions, beta versions or release candidates, as long as the	(21) In order to ensure that manufacturers can release software for testing purposes before subjecting their products to conformity assessment, Member States should not prevent the making available of unfinished software, such as alpha versions, beta versions or release candidates, as long as the version is only made available for	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	the time necessary to test it and gather feedback. Manufacturers should ensure that software made available under these conditions is only released following a risk assessment and that it complies to the extent possible with the security requirements relating to the properties of products with digital elements imposed by this Regulation. Manufacturers should also implement the vulnerability handling requirements to the extent possible. Manufacturers should not force users to upgrade to versions only released for testing purposes.	version is only made available for the time necessary to test it and gather feedback. Manufacturers should ensure that software made available under these conditions is only released following a risk assessment and that it complies to the extent possible with the security requirements relating to the properties of products with digital elements imposed by this Regulation. Manufacturers should also implement the vulnerability handling requirements to the extent possible. Manufacturers should not force users to upgrade to versions only released for testing purposes.	the time necessary to test it and gather feedback. Manufacturers should ensure that software made available under these conditions is only released following a risk assessment and that it complies to the extent possible with the security requirements relating to the properties of products with digital elements imposed by this Regulation. Manufacturers should also implement the vulnerability handling requirements to the extent possible. Manufacturers should not force users to upgrade to versions only released for testing purposes.	
Recital 22				
32	(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	(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, <u>necessary security updates</u> , software updates or repairs ~~could be assimilated to~~	(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. These essential requirements, including vulnerability management handling requirements, apply to each individual product with digital elements when placed on the market, irrespective of whether the product with digital elements is manufactured as an individual unit or in series. For example, for	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	~~maintenance operations~~ <u>such as minor adjustment of the source code that can improve the security, should not be considered to be substantial modifications</u>, 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. <u>This is generally the case for new software versions which aim at improving performance and fixing vulnerabilities. Minor functionality updates, such as visual enhancements, the addition of new languages to the user interface or of a new set of pictograms, should generally not be considered to be substantial modifications.</u> 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, <u>as is generally the case for software revisions. The Commission should issue</u>	a product type, each individual product with digital elements should have received all security patches or updates available to address relevant security issues at the time when it is placed on the market. When the products are subsequently modified, by physical or digital means, in a way that is not foreseen by the manufacturer and that may imply that they no longer meet the relevant essential requirements, the modification should be considered as substantial. For example, software updates or repairs could be assimilated to maintenance operations provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended ~~use~~purpose for which the product has been assessed may be changed. As is the case for physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where- the software update modifies the ~~original~~ intended functions, type or performance of ~~the~~purpose of that product and these changes were not foreseen in the initial risk assessment, or where the nature of the hazard has changed or the level of risk has increased because of the software update, and	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>guidelines on how to determine what constitutes a substantial modification.</u>	the product is made available on the market.	
Recital 22a				
32a			(22a) Where security updates, which are designed to decrease the level of risk of a product with digital elements, do not modify the intended purpose of a product, they are not considered a substantial modification. For example, this could be the case where a security update addresses a known vulnerability, including by modifying functions or the performance of a product with digital elements for the sole purpose of decreasing the level of cybersecurity risk. Conversely, where feature updates modify the original intended functions or the type or performance of a product for purposes other than merely decreasing the level of cybersecurity risk, they should be considered a substantial modification, as the addition of new features typically leads to a broader attack surface, thereby increasing the risk. For example, this could be the case where a new input element is added to an application, requiring the manufacturer to ensure adequate	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			input validation. In assessing whether a feature update is considered a substantial modification it is not relevant whether it is provided as a separate update or in combination with a security update.	
Recital 23				
33	(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, 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, 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, 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. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 24				
34	(24) Refurbishing, maintaining and repairing of a product with digital elements, as defined in the Regulation [Eco-design Regulation], does not necessarily lead to a substantial modification of the product, for instance if the intended use and functionalities are not changed and the level of risk remains unaffected. However, upgrading a product by the manufacturer might lead to changes in the design and development of the product and therefore might affect the intended use and the compliance of the product with the requirements set out in this Regulation.	(24) Refurbishing, maintaining and repairing of a product with digital elements, as defined in the Regulation [Eco-design Regulation], does not necessarily lead to a substantial modification of the product, for instance if the intended use and functionalities are not changed and the level of risk remains unaffected. However, upgrading a product by the manufacturer might lead to changes in the design and development of the product and therefore might affect the intended use and the compliance of the product with the requirements set out in this Regulation.	(24) Refurbishing, maintaining and repairing of a product with digital elements, as defined in the Regulation [Eco-design Regulation], does not necessarily lead to a substantial modification of the product, for instance if the intended ~~use~~ purpose and functionalities are not changed and the level of risk remains unaffected. However, upgrading a product by the manufacturer might lead to changes in the design and development of the product and therefore might affect the intended ~~use~~ purpose and the compliance of the product with the requirements set out in this Regulation.	
Recital 25				
35	(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	(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	(25) Products with digital elements should be ~~considered critical~~ included in Annex III of this Regulation 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 a function having a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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 EU)]~~ , or for <u>2022/2555</u> , or the performance of critical or sensitive functions, ~~such as processing of personal data~~ <u>that have an impact on health, safety or fundamental rights</u> .	products with digital elements through direct manipulation, such as a central system function , or the intended use. In particular, vulnerabilities in products with digital elements that have a cybersecurity-related functionality, such as secure elements, can lead to a propagation of security issues throughout the supply chain. The severity of the impact of a cybersecurity incident may also increase when taking into account the intended use of the product, such as in an industrial setting or in the context of an essential entity of the type referred to in Annex [Annex I] to Directive [Directive XXX/ XXXX (NIS2)], or for the performance of critical or sensitive functions, such as primarily performs a central system function, including network management, configuration control, virtualisation or processing of personal data.	
Recital 26				
36	(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,	(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,	(26) ~~Critical~~ Certain categories of products with digital elements should be subject to stricter conformity assessment procedures, while keeping a proportionate approach. For this purpose, those categories of critical products with	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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~~ high risk environments, and therefore should undergo a stricter conformity assessment procedure.	digital elements should be divided into two classes, reflecting the level of cybersecurity risk linked to these categories of products. The categories of products with digital elements listed in class I of Annex III to this Regulation either have a cybersecurity-related functionality or a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation, such as a central system function. The categories of products with digital elements listed in class II of Annex III meet both these criteria. Cumulating these criteria indicates that a potential cyber incident involving products in class II might lead to greater negative impacts than an incident involving products in class I, for instance due to the nature of their cybersecurity-related function or intended use in sensitive environments and the performance of a function which carries a significant risk of adverse effects, such as a central system function , and therefore should undergo a stricter conformity assessment procedure.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 27				
37	(27) The categories of critical products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation lists products which are defined by their core functionality as general purpose microprocessors in class II. As a result, general purpose microprocessors are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a general purpose microprocessor. The Commission should adopt delegated acts [by 12 months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III.	(27) The categories of critical products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation lists products which are defined by their core functionality as general purpose microprocessors in class ~~II~~. As a result, general purpose microprocessors are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a general purpose microprocessor. The Commission should adopt delegated acts [by ~~12~~6 months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III. <u>In order to ensure legal clarity and certainty as well as predictability for stakeholders to comply with this Regulation, amendments to the list in Annex III should be made at the earliest two years after the entry into force of this Regulation and again at the earliest two years thereafter. The Commission should establish a process under which a</u>	(27) The categories of critical products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation lists products which are defined by their core functionality as firewalls, intrusion detection or prevention systems-general purpose microprocessors in class II. As a result, firewalls, intrusion detection or prevention systems general purpose microprocessors are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate firewalls, intrusion detection or prevention systems-a general purpose microprocessor. The Commission should adopt an implementing act [~~delegated acts~~ [by 12 months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>product which is a candidate to be a critical product can be reviewed in a collaborative process by all relevant stakeholders, including manufacturers and users, to assess the security risk posed by potential cybersecurity issues with the product, whether and how much designating the product as critical would likely reduce that risk, and the costs associated with designating the product as critical, before adopting the relevant delegated acts.</u>		
Recital 27a				
37a			(27a) The categories of products with digital elements listed in Annex IIIa to this Regulation have a cybersecurity-related functionality and primarily perform a central system function or a function having the potential to disrupt, control or damage a large number of other products with digital elements through direct manipulation. Furthermore, those product categories are considered to be critical dependencies for entities of a type referred to in Annex I to Directive (EU) 2022/2555. The categories of products with digital elements listed in Annex IIIa to this Regulation, due to their criticality,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			already widely use various forms of certification, and are also covered by the European Common Criteria-based cybersecurity certification scheme set out in the [Commission Implementing Regulation (EU) No .../... of XXX on the European Common Criteria-based cybersecurity certification scheme] (EUCC). Therefore, in order to ensure a common adequate cybersecurity protection of these products with digital elements in the Union, it could be adequate and proportionate to subject these products, by means of a delegated act, to mandatory European cybersecurity certification where a relevant certification scheme covering those products is already in place and an impact assessment has been carried out by the Commission. The assessment of the potential market impact of the envisaged mandatory certification should consider both the supply and demand side, including whether there is sufficient demand for the products with digital elements concerned from both Member States and users, for European cybersecurity certification to be required, as well as the purposes for which the products are intended to be used, such as critical dependencies by	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			entities of a type referred to in Annex I to Directive (EU) 2022/2555. The impact assessment should also analyse the potential effects of the mandatory certification on the availability of those products on the internal market, as well as the supply and demand side and the capabilities and the readiness of the Member States for the implementation of the relevant European cybersecurity certification schemes.	
Recital 27aa				
37b			(27aa) Delegated acts requiring mandatory European cybersecurity certification should specify the products with digital elements that have the core functionality of a product category listed in Annex IIIa that are to be subject to mandatory certification, as well as the assurance level required. The required assurance level should be proportionate to the level of cybersecurity risk associated with the product with digital elements. For instance, where the product has the core functionality of a product category listed in Annex IIIa and is intended for the use in a sensitive or critical environment, such as	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			products intended for the use of entities of a type referred to in Annex I to Directive (EU) 2022/2555, it may require the highest assurance level.	
Recital 27b				
37c			(27b) In order to ensure a common adequate cybersecurity protection in the Union of products with digital elements that have the core functionality of a product category listed in Annex IIIa, the Commission should also be empowered to adopt delegated acts to amend Annex IIIa by adding further or removing categories of products with digital elements for which the manufacturers could be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with this Regulation. A new category of products with digital elements can be added to those categories if there is a critical dependency on it of entities of a type referred to in Annex I to Directive (EU) 2022/2555 or, if affected by cybersecurity incidents or when containing exploited	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			vulnerabilities, this can lead to disruptions for critical supply chains. When assessing the need for adding or removing categories of products with digital elements by means of a delegated act, the Commission may take into account whether the Member States identified at national level products with digital elements that have a critical role for the resilience of entities of a type referred to in Annex I to Directive (EU) 2022/2555 and which increasingly face supply chain cyber attacks, with potential serious disruptive effects. Furthermore, the Commission may take into account the outcome of the Union level coordinated security risk assessment of critical supply chains as per Article 22 of Directive (EU) 2022/2555.	
Recital 27a				
37d		<u>(27a) The Commission should set up an expert group on cyber resilience (the ‘Expert Group’), with a wide and diverse membership. The Expert Group should support the Commission in order to ensure the proper implementation of this Regulation, for example by advising the Commission on possible</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>amendments to the list of critical products set out in Annex III or by analysing in what way European and international standards can enable compliance with the essential requirements of this Regulation. The Commission should consult the Expert Group and carry out public consultations while preparing delegated and implementing acts pursuant to this Regulation, in order to ensure that all stakeholders can provide the necessary input.</u>		
Recital 28				
38	(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	(28) This Regulation addresses cybersecurity risks in a targeted manner. Products with digital elements might, however, pose other safety risks, that are not <u>always</u> related to cybersecurity <u>but can be a consequence of a security breach</u> . 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]~~ <u>(EU) 2023/988</u> . 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~~	(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~~ harmonisation legislation. If no other Union harmonisation legislation is applicable, they should be subject to Regulation ~~[General Product Safety Regulation]~~ (EU) 2023/988 of the European Parliament and of the Council¹ . Therefore, in light of the targeted nature of this Regulation, as a derogation from Article 2(1), third subparagraph, point (b), of	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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].	~~Regulation~~ (EU) 2023/988 , Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation ~~[General Product Safety Regulation]~~ (EU) 2023/988 should apply to products with digital elements with respect to safety risks not covered by this Regulation, if those products are not subject to specific requirements imposed by other Union harmonisation legislation within the meaning of ~~[Article 3, point (25) of the General Product Safety Regulation]~~ Regulation (EU) 2023/988 .	Regulation ~~[General Product Safety Regulation]~~ (EU) 2023/988 , 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 [as defined in Article 3, point (25) of the General Product Safety Regulation]~~ Regulation (EU) 2023/988 . 1. Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).	
Recital 29				
39	(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation ¹ [the AI Regulation] which fall within the scope of this Regulation should comply with the essential requirements set out in this	(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation ¹ [the AI Regulation] which fall within the scope of this Regulation should comply with the essential requirements set out in this	(29) Products with digital elements classified as high-risk AI systems according to Article 6 of Regulation ¹ [the AI Regulation] which fall within the scope of this Regulation should comply with the essential requirements set out in this	

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

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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. 1. Regulation [the AI Regulation].	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. 1. Regulation [the AI Regulation].	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. 1. Regulation [the AI Regulation].	
Recital 30				
40	(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	(30) The machinery products falling within the scope of Regulation ~~[Machinery Regulation proposal]~~ <u>(EU) 2023/1230 of the European Parliament and of the Council¹</u> 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]~~ <u>(EU) 2023/1230</u>, as regards protection	(30) To the extent that ~~The machinery~~ products falling within the scope of Regulation ~~[Machinery Regulation proposal]~~ <u>(EU) 2023/1230 of the European Parliament and of the Council¹</u> are products with digital elements within the meaning of this Regulation, manufacturers of these products should comply with both the essential requirements established by this Regulation and the essential health and safety requirements set out in Regulation (EU) 2023/1230. The essential requirements under and for which a declaration of conformity has been	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	with those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.	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. <u>1. Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (OJ L 165, 29.6.2023, p. 1).</u>	issued on the basis of this Regulation should be deemed to be in conformity and certain essential requirements of Regulation (EU) 2023/1230 might address similar aspects. For instance, compliance with the essential health requirements under this Regulation could facilitate the compliance with the essential requirements related to cybersecurity regarding the protection against corruption and safety requirements and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to Regulation (EU) 2023/1230. A manufacturer may identify such synergies during the risk assessment process as foreseen under Regulation (EU) 2023/1230. Furthermore, the Commission and the European Standardisation Organisations should take into account this Regulation in the preparation and development of harmonised standards to facilitate the implementation of sections 1.1.9 and 1.2.1 of the Regulation [Machinery Regulation proposal], (EU) 2023/1230 as regards in particular the cybersecurity aspects related to the protection against corruption and safety and reliability of control systems in so far as the compliance with those requirements is demonstrated by the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			EU declaration of conformity issued under this set out in Sections 1.1.9 and 1.2.1 of Annex III to that Regulation. 1. Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (OJ L 165, 29.6.2023, p. 1).	
Recital 31				
41	(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	(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	(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	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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~~ <u>not do not fall</u> within the scope of this Regulation, as they are not placed on the market.	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.	
Recital 32				
42	(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	(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~~ <u>throughout the support period</u> , 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	(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~~ <u>lifecycle</u> , 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	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	identify relevant risks and relevant essential requirements and in order to appropriately apply suitable harmonised standards or common specifications.	product with digital elements to identify relevant risks and relevant essential requirements and in order to <u>make available their products without known exploitable vulnerabilities that might have an impact on the security of those products and to</u> appropriately apply suitable harmonised standards, <u>common specifications or international standards</u> ~~or common specifications~~ .	identify relevant risks and relevant essential requirements and in order to appropriately apply suitable harmonised standards or common specifications.	
Recital 32a				
42a			(32a) When assessing the risks associated with a product with digital elements, manufacturers should take into account the potential systemic impact of a vulnerability on consumers and organisations. Where a product with digital elements is used only by a limited number of users or in less critical or sensitive environments, as it is often the case with products with digital elements placed on the market by micro and small enterprises, manufacturers should be able to consider the risk of such a systemic impact as low.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 32aa				
42b			(32aa) Where certain essential requirements are not applicable to a product with digital elements, the manufacturer should include a clear justification in the cybersecurity risk assessment included in the technical documentation. This could be the case where an essential requirement would be incompatible with the nature of a product with digital elements. For example, the intended purpose of a product may require the manufacturer to follow widely recognised interoperability standards even if their security features are no longer considered state of the art. Similarly, other Union legislation may require manufacturers to apply specific interoperability requirements. This is for example the case of Commission Implementing Regulation (EU) 2019/838 on technical specifications for vessel tracking and tracing systems and repealing Regulation (EC) No 415/2007, which specifies how AIS transponders should communicate with one another. Where an essential requirement is not applicable to a product with digital elements, but the manufacturer has identified	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			cybersecurity risks in relation to this essential requirement, it should take measures to address those risks by other means, for instance by limiting the intended purpose of the product to trusted environments or by informing the users about those risks.	
Recital 32a				
42c		<u>(32a) Manufacturers should determine the support period during which they ensure that vulnerabilities are handled, duly taking into account various criteria, including the expected product lifetime, the nature of the product itself, the availability of the operating environment, the expectations of users, particularly consumers, and, where possible, the support period of other main components integrated into the product. Manufacturers should ensure that the support period adequately reflects the need to promote cybersecurity in the Union's market and is set with due consideration of the period during which a product with digital elements is expected to be available on the market. Market surveillance authorities should proactively ensure that manufacturers apply these criteria in an adequate</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>manner. Market surveillance authorities and the Commission should collect and analyse data about the support periods set by manufacturers and the expected product lifetimes, in order to ensure that this Regulation meets its goal of promoting the cybersecurity of products with digital elements. Such analyses should, inter alia, inform the Commission's evaluation of this Regulation, once it applies.</u>		
Recital 32b				
42d		<u>(32b) Manufacturers should ensure, where technically feasible, that products with digital elements clearly differentiate between security and functionality updates. Security updates, designed to decrease the level of risk or to remedy potential vulnerabilities, should be installed automatically, in particular in the case of consumer products. Users should retain the possibility to de-activate this feature, with a clear and easy-to-use mechanism. Once the manufacturer no longer ensures that vulnerabilities of the product with digital elements are handled, it should inform users in a simple and clear manner, for example via the display of a user-friendly</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>notification.</u>		
Recital 32c				
42e		<u>(32c) Where manufacturers set a support period of shorter than five years and no longer offer vulnerability handling for the product with digital elements, they should be able to make their source code available to undertakings that wish to provide security updates and other similar services. Such access should be made available only as part of a contractual arrangement that protects the ownership of the product with digital elements and prevents the dissemination of the source code to the public, except where such code has already been provided under a free and open-source licence.</u>		
Recital 33				
43	(33) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential requirements. These essential requirements should be without prejudice to the EU coordinated risk assessments of critical supply chains established by [Article X] of Directive [Directive	(33) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential requirements. These essential requirements should be without prejudice to the EU coordinated risk assessments of critical supply chains established by ~~Article X~~ of Directive ~~Directive~~	(33) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential requirements. These essential requirements should be without prejudice to the ~~EU~~ Union level coordinated security risk assessments of critical supply chains established by ~~pursuant to~~ Article	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	XXX/XXXX(NIS2)]¹, which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, it should be without prejudice to the Member States' prerogatives to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Recommendation (EU) 2019/534, in the Union-wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the NIS Cooperation Group as referred to in [Directive XXX/XXXX (NIS2)]. 1. Directive XXX of the European Parliament and of the Council of [date] [on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ L xx, date, p.x)].	~~XXX/XXXX(NIS2)]¹~~ (EU) 2022/2555, which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, it should be without prejudice to the Member States' prerogatives to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Recommendation (EU) 2019/534, in the Union-wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the NIS Cooperation Group as referred to in ~~[Directive XXX/XXXX (NIS2EU)]¹~~ 2022/2555. ~~1. Directive XXX of the European Parliament and of the Council of [date] [on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ L xx, date, p.x)].~~	~~X]22 of Directive [Directive XXX/XXXX(NIS2)]¹~~ (EU) 2022/2555, which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, it should be without prejudice to the Member States' prerogatives to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Recommendation (EU) 2019/534, in the ~~Union-wide~~ EU coordinated risk assessment of ~~5G networks security~~ the cybersecurity of 5G networks and in the EU Toolbox on 5G cybersecurity agreed by the NIS Cooperation Group established under ~~as referred to in [Directive XXX/XXXX (NIS2EU)]¹~~ 2022/2555. ~~1. Directive XXX of the European Parliament and of the Council of [date] [on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ L xx, date, p.x)].~~	
Recital 33-a				
43a			(33-a) For the purpose of ensuring the security of products with digital elements after their placing on the market, manufacturers should determine the expected	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			product lifetime. To that end, manufacturers should take into account the time users reasonably expect to be able to use the product with digital elements given its functionality and intended purpose and therefore can expect to receive security updates. In addition, manufacturers should also be able to take into account other elements, such as relevant Union law determining the lifetime of products with digital elements; the nature of the product with digital elements, including the licensing terms under which it is made available; the expected availability of the operating environment the product with digital elements is intended for; the lifetime of products with digital elements offering a similar functionality placed on the market by other manufacturers, including, where available, relevant guidance provided by market surveillance authorities; as well as the lifetime of integrated components that provide core functions and are sourced from third parties.	
Recital 33a				
43b			(33a) To ensure that the expected product lifetime specified by	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			manufacturers is sufficiently aligned within each category of products with digital elements, market surveillance authorities, through the dedicated administrative cooperation group (ADCO) established by this Regulation, should consider publishing, with the support of the Commission, statistics about the average expected product lifetime, as specified by manufacturers, per category of products with digital elements.	
Recital 34				
44	(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of Directive [Directive XX/XXXX (NIS2)] are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product	(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)]~~ <u>2022/2555</u> are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product	(34) To ensure that the national CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 have an adequate overview of the vulnerabilities exploited by malicious actors in products with digital elements and ~~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 as set out in Directive (EU) 2022/2555 and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should ~~also consider disclosing~~ disclose fixed vulnerabilities to the European vulnerability database established under Directive ~~[Directive XX/XXXX (NIS2EU)]~~ 2022/2555 and managed by ENISA. <u>ENISA should also publish notified vulnerabilities in the European vulnerability database and should have in place an appropriate procedure regarding the publication process in order to give manufacturers the time to develop the necessary security updates and users the time to implement them or take other corrective or mitigating measures. The European-or under any other publicly accessible</u> vulnerability database <u>should assist manufacturers in detecting known exploitable vulnerabilities found in their products, in order to ensure that secure products are placed on the market.</u>	manufacturers of products with digital elements should notify ~~to~~ ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under Directive ~~[Directive XX/XXXX (NIS2EU)]~~ 2022/2555 and managed by ENISA or under any other publicly accessible vulnerability database, as well as machine-readable advisories.	
Recital 34a				
44a		<u>(34a) The Union needs to maximise the benefits of its economic openness while minimising the risks from economic dependencies on high-risk vendors.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>through a common strategic framework for Union economic security¹. Dependencies on high-risk suppliers of critical products with digital elements pose a strategic risk that should be addressed at Union level, especially when the critical products with digital elements are intended for the use by essential entities of the type referred to in Directive (EU) 2022/2555. Such risks may be linked to the jurisdiction applicable to the manufacturer, the characteristics of its corporate ownership and the links of control to a third-country government where it is established, in particular whether a country engages in economic espionage and its legislation obliges arbitrary access to any kind of company operations or data, including commercially sensitive data, and can impose obligations for intelligence purposes without democratic checks and balances, oversight mechanism, due process or the right to appeal to an independent judiciary. Market surveillance authorities and the Commission should provide guidance and targeted recommendations to economic operators in order to ensure that appropriate corrective actions are put in place where there is sufficient reason to consider that</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u><i>a product with digital elements presents a significant cybersecurity risk in light of such non-technical risk factors.</i></u> <u><i>1. See JOIN (2023)20 Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy".</i></u>		
Recital 35				
45	(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,	(35) Manufacturers should also report to ENISA any <u>significant</u> incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive ~~f~~ Directive ~~XXX/XXXX~~ ~~(NIS2EU)~~ <u>2022/2555</u> 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 ~~f~~ Directive ~~XXX/XXXX~~ ~~(NIS2EU)~~ <u>2022/2555</u> 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 <u>significant</u> incidents having an impact on the security of their products with digital elements, manufacturers should also	(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,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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.	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.	
Recital 35a				
45a			(35a) In exceptional circumstances, the initial recipient of a notification should be able to decide to delay its dissemination via the single reporting platform where this can be justified on cybersecurity related grounds and for a period of time that is strictly necessary, in particular where manufacturers demonstrate that such a delay is justified. The CSIRTs network should develop specifications on the terms and conditions for when cybersecurity related grounds could be applied. Examples of cybersecurity related grounds include an ongoing coordinated vulnerability disclosure procedure or situations in which a manufacturer is expected to provide a mitigating measure shortly and the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			cybersecurity risks of an immediate dissemination via the platform outweigh its benefits.	
Recital 35b				
45b			(35b) In order to simplify the reporting of information required under this Regulation, in consideration of other complementary reporting requirements laid down in other Union law, such as Directive (EU) 2022/2555, Regulation (EU) 2016/679 and Directive 2002/58/EC, as well as in order to decrease the administrative burden for entities, Member States are encouraged to consider providing at national level single entry points for such reporting requirements. The use of such national single entry points for the reporting of security incidents under Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to the independence of the authorities referred to therein. When establishing the single reporting platform referred in this Regulation, ENISA, following the specifications of the CSIRTs	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			network, should also take into account the possibility for the national electronic notification end-points referred to in this Regulation to be integrated into national single entry points that may also integrate other notifications required by other Union law.	
Recital 35c				
45c			(35c) When establishing the single reporting platform referred in this Regulation, ENISA, following the specifications of the CSIRTs network, should analyse potential complementarities with the European vulnerability database established in accordance with Article 12(2) of Directive (EU) 2022/2555.	
Recital 35a				
45d		<u>(35a) Manufacturers and other entities and actors should also be able to report to ENISA, on a voluntary basis, about other cybersecurity incidents, cyber threats, near misses and any other vulnerability.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 35b				
45e		<u>(35b) ENISA should establish a secure digital reporting mechanism that, in order to simplify reporting for manufacturers, should serve as a single entry point for reporting obligations established under this Regulation. Manufacturers of products with digital elements are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. The mechanism could, where possible, allow other Union law such as Regulation (EU) 2016/679, Directive (EU) 2022/2555 and Directive 2002/58/EC of the European Parliament and of the Council¹ to be reported through the same mechanism. The mechanism may also be used for the voluntary notifications by manufacturers and other entities and actors. ENISA should ensure that they have procedures in place to handle classified information in a secure and confidential manner.</u> <u>1. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37).</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 35c				
45f		<u>(35c) Entities and natural persons researching vulnerabilities may in some Member States be exposed to criminal and civil liability. The Commission should issue guidelines with regard to the non-prosecution of information security researchers and an exemption from civil liability for those activities.</u>		
Recital 36				
46	(36) Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities. A coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, manufacturers of such	(36) Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities <u>either directly to the manufacturer or indirectly, and where requested anonymously, via CSIRTs designated as a coordinator for the purposes of coordinated vulnerability disclosure in accordance with Article 12(1) of Directive (EU) 2022/2555.</u> ~~A~~ coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such	(36) Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities. A coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Moreover, manufacturers should also consider publishing their security policies in machine-readable format. Given the fact that information about exploitable vulnerabilities in widely used	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts (so-called ‘bug bounty programmes’).	vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, manufacturers of such products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts (so-called ‘bug bounty programmes’).	products with digital elements can be sold at high prices on the black market, manufacturers of such products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts (so-called ‘bug bounty programmes’).	
Recital 36a				
46a		<u>(36a) Member States and ENISA should make sure that vulnerabilities reported under this Regulation are not used by public bodies for intelligence, surveillance or offensive purposes.</u>		
Recital 37				
47	(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements,	(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements,	(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties.	including by drawing up a software bill of materials <u>(SBOMs). A SBOM—A software bill of materials</u> can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties. <u>Manufacturer should not, however, be obliged to make the software bill of materials public, as this may have unintended consequences on the cybersecurity of their products with digital elements.</u>	including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties.	
Recital 37a				
47a			(37a) Under the new complex business models linked to online sales, the same entity can provide a variety of services. Depending on the nature of the services provided in relation to a given product with digital elements, the same entity may fall within different categories of business models. Where an entity provides only online intermediation services for	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			a given product with digital elements and is merely a provider of an online marketplace, as defined by Article 3, point (14), of Regulation (EU) 2023/988, it would not qualify as one of the types of economic operator defined in this Regulation. A provider of an online marketplace means a provider of an intermediary service using an online interface, which allows consumers to conclude distance contracts with traders for the sale of products, while online interface means any software, including a website, part of a website or an application, including mobile applications. In case the same entity is a provider of an online marketplace and also acts as an economic operator as defined in this Regulation for the sale of particular products with digital elements, it would qualify also as the relevant type of economic operator for the purposes of this Regulation. In such a case, the entity in question would therefore have to comply with the obligations laid down in this Regulation for the relevant type of economic operator. For instance, if the provider of the online marketplace also distributes a product with digital elements, then, with respect to the sale of	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			that product, it would be considered to be a distributor. Similarly, if the entity in question sells its own branded products with digital elements, it would qualify as a manufacturer and would thus have to comply with the applicable requirements for manufacturers. Also some entities can qualify as fulfilment service providers as defined by Article 3(11) of Regulation (EU) 2019/1020 if they offer such services. Such cases would need to be assessed on a case-by-case basis.	
Recital 38				
48	(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 ¹ . Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do	(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 ¹ . Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do	(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 ¹ . Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	not entirely satisfy the requirements of this Regulation. 1. 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).	not entirely satisfy the requirements of this Regulation. <u>The standardisation process should ensure a balanced representation of interests and effective participation of civil society stakeholders, including consumer organisations. International standards should also be taken into account, in order to simplify the development of harmonised standards and the implementation of this Regulation, as well as to reduce non-tariff technical barriers to trade.</u> 1. 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).	not entirely satisfy the requirements of this Regulation. 1. 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).	
Recital 38a				
48a		<u>(38a) Considering the broad scope of this Regulation, the timely development of harmonised standards poses a significant challenge. The Commission should ensure that harmonised standards will be in place by the date of</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>application of this Regulation, in order to ensure the successful implementation of this Regulation.</u>		
Recital 39				
49	(39) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, processes and services. European cybersecurity certification schemes can cover products with digital elements covered by this Regulation. This Regulation should create synergies with Regulation (EU) 2019/881. In order to facilitate the assessment of conformity with the requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and which has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity certification schemes for products with digital elements should be	(39) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, processes and services. European cybersecurity certification schemes can ~~cover~~ <u>provide a common framework of trust for users to use</u> products with digital elements covered by this Regulation. This Regulation should <u>consequently</u> create synergies with Regulation (EU) 2019/881. In order to facilitate the assessment of conformity with the requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and which has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity	(39) Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, processes and services. European cybersecurity certification schemes can cover products with digital elements covered by this Regulation. This Regulation should create synergies with Regulation (EU) 2019/881. In order to facilitate the assessment of conformity with the requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and which has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential requirements of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity certification schemes for products with digital elements should be	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	assessed in the light of this Regulation. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation. The Commission should be empowered to specify, by means of implementing acts, the European cybersecurity certification schemes that can be used to demonstrate conformity with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, where applicable, the Commission should specify if a cybersecurity certificate issued under such European cybersecurity certification schemes eliminates the obligation for manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements.	certification schemes for products with digital elements should be assessed in the light of this Regulation. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation. The Commission should be empowered to specify, by means of ~~implementing~~ <u>delegated</u> acts, the European cybersecurity certification schemes that can be used to demonstrate conformity <u>for products with digital elements</u> with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, ~~where applicable, the Commission there should specify if a cybersecurity certificate issued under such European cybersecurity certification schemes eliminates the~~ <u>be no</u> obligation for manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements <u>where a cybersecurity certificate has been issued under such European cybersecurity certification schemes, at a substantial or high level.</u>	assessed in the light of this Regulation. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential requirements and conformity assessment procedures as set out in this Regulation and facilitate compliance with this Regulation. ~~The Commission should be empowered to specify, by means of implementing acts, the~~ For European cybersecurity certification schemes that ~~can be used to demonstrate conformity with the essential requirements set out in this Regulation. Furthermore, in order to avoid undue administrative burden for manufacturers, where applicable,~~ enter into force before the entry into force of this Regulation, further specifications by means of implementing acts may be needed on detailed aspects of how a presumption of conformity can apply. The Commission should be empowered to specify, by means of implementing acts, if a cybersecurity certificate issued under such which conditions the European cybersecurity certification schemes can be used to demonstrate conformity with the essential requirements set out in ~~eliminates the obligation for~~	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			manufacturers to carry out a third-party conformity assessment as provided by this Regulation for corresponding requirements.	
Recital 39a				
49a		<u>(39a) In order to facilitate the compliance with this Regulation, the Commission should update the Union rolling work programme and request ENISA to prepare the missing candidate schemes in accordance with Article 48 of Regulation (EU) 2019/881.</u>		
Recital 40				
50	(40) Upon entry into force of the implementing act setting out the [Commission Implementing Regulation (EU) No .../... of XXX on the European Common Criteria-based cybersecurity certification scheme] (EUCC) which concerns hardware products covered by this Regulation, such as hardware security modules and microprocessors, the Commission may specify, by means of an implementing act, how the EUCC provides a presumption of conformity with the essential requirements as referred to in Annex I of this Regulation or parts thereof.	(40) Upon entry into force of the implementing act setting out the [Commission Implementing Regulation (EU) No .../... of XXX on the European Common Criteria-based cybersecurity certification scheme] (EUCC) which concerns hardware products covered by this Regulation, such as hardware security modules and microprocessors, the Commission may specify, by means of an implementing act, how the EUCC provides a presumption of conformity with the essential requirements as referred to in Annex I of this Regulation or parts thereof.	(40) Upon entry into force of the implementing act setting out the [Commission Implementing Regulation (EU) No .../... of XXX on the European Common Criteria-based cybersecurity certification scheme] (EUCC) which concerns ~~hardware~~ products covered by this Regulation, such as hardware security modules and microprocessors, the Commission may specify, by means of an implementing act, how the EUCC provides a presumption of conformity with the essential requirements as referred to in Annex I of this Regulation or parts thereof.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Furthermore, such implementing act may specify how a certificate issued under the EUCC eliminates the obligation for manufacturers to carry out a third-party assessment as requested by this Regulation for corresponding requirements.	Furthermore, such implementing act may specify how a certificate issued under the EUCC eliminates the obligation for manufacturers to carry out a third-party assessment as requested by this Regulation for corresponding requirements.	Furthermore, such implementing act may specify how a certificate issued under the EUCC eliminates the obligation for manufacturers to carry out a third-party assessment as requested by this Regulation for corresponding requirements.	
Recital 41				
51	(41) Where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation request by any of the European standardisation organisations, undue delays in the establishment of appropriate harmonised standards, or a lack of compliance of developed standards with the requirements of this Regulation or with a request of the Commission. In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with	(41) Where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of ~~implementing acts. Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of the standardisation request by any of the European standardisation organisations,~~ <u>delegated acts, after taking into account international standards. Such an option should be seen as an exceptional ‘fall back’ solution, where the standardisation process is blocked, where there are</u> undue delays in the establishment of appropriate harmonised standards, or ~~a lack of compliance of developed standards~~ <u>where the deliverables fail to comply</u> with the ~~requirements of~~	(41) ~~Where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. Reasons for developing such common specifications, instead of relying on harmonised~~ The current EU standardisation framework which is based on the New Approach principles set out in Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards and on Regulation (EU) No 1025/2012 represents the framework by default to elaborate standards that provide for a presumption of conformity with the relevant essential requirements of this Regulation. European standards should be market-driven, take into account the public interest, as well	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.	~~this Regulation or with a~~<u>initial</u> request of the Commission. In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.	as the policy objectives clearly stated in the Commission's, might include a refusal of the standardisation request by any of the to one or more European standardisation organisations to draft harmonised standards, within a set deadline and be based on consensus. However, ,undue delays in the establishment of appropriateabsence of relevant references to harmonised standards, the Commission should be able to adopt implementing acts establishing common specifications for the essential cybersecurity-or a lack of compliance of developed standards with the requirements of this Regulation, provided that in doing so it duly respects the role and functions of standardisation organisations, as an exceptional fall back solution-or with a request of the Commission. In order to facilitate assessment of conformity with the essentialthe manufacturer's obligation to comply with those cybersecurity requirements, when the standardisation process is blocked or when laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements are delays in the establishment of appropriate harmonised standards. If such delay is due to the technical complexity of the standard in question, this should be considered by the Commission before contemplating the establishment of common specifications.	
Recital 41a				
51a			(41a) With a view to establishing, in the most efficient way, common specifications that cover the essential requirements of this Regulation, the Commission should involve relevant stakeholders in the process.	
Recital 41b				
51b			(41b) Reasonable period should mean, in relation to the publication of reference to harmonised standards in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012, a period during which the publication in the Official Journal	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			of the European Union of the reference to the standard, its corrigendum or its amendment is expected and which should not exceed one year after the deadline for drafting a European standard set in accordance with Regulation (EU) No 1025/2012.	
Recital 41c				
51c			(41c) In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements. Text corresponds to Commission text of recital 41, last sentence.	
Recital 41d				
51d			(41d) The application of harmonised standards or of other available means providing presumption of conformity in relation to the essential	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			requirements applicable to the products with digital elements will facilitate the assessment of conformity by the manufacturer. If the manufacturers chooses not to apply such means for certain requirements, they have to indicate in their technical documentation how the compliance is reached otherwise. Furthermore, the application of harmonised standards or of other available means providing presumption of conformity by manufacturers would facilitate the check of compliance of products with digital elements by market surveillance authorities. Therefore, manufacturers of products with digital elements are encouraged to apply harmonised standards or other available means providing presumption of conformity to demonstrate conformity with the essential requirements of this Regulation.	
Recital 42				
52	(42) Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential requirements of this Regulation and, where applicable, of	(42) Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential requirements of this Regulation and, where applicable, of	(42) Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential requirements of this Regulation and, where applicable, of	(42) Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential requirements of this Regulation and, where applicable, of

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	the other relevant Union harmonisation legislation by which the product is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legislation. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.	the other relevant Union harmonisation legislation by which the product is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legislation. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.	the other relevant Union harmonisation legislation by which the product is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legislation. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.	the other relevant Union harmonisation legislation by which the product is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legislation. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity. Text Origin: Commission Proposal
Recital 43				
53	(43) The CE marking, indicating the conformity of a product, is the visible consequence of a whole process comprising conformity assessment in a broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council¹. Rules governing the affixing of the CE marking on products with digital	(43) The CE marking, indicating the conformity of a product, is the visible consequence of a whole process comprising conformity assessment in a broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council¹. Rules governing the affixing of the CE marking on products with digital	(43) The CE marking, indicating the conformity of a product, is the visible consequence of a whole process comprising conformity assessment in a broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council¹. Rules governing the affixing of the CE marking on products with digital	(43) The CE marking, indicating the conformity of a product, is the visible consequence of a whole process comprising conformity assessment in a broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council¹. Rules governing the affixing of the CE marking on products with digital

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	elements should be laid down in this Regulation. The CE marking should be the only marking which guarantees that products with digital elements comply with the requirements of this Regulation. 1. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).	elements should be laid down in this Regulation. The CE marking should be the only marking which guarantees that products with digital elements comply with the requirements of this Regulation. 1. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).	elements should be laid down in this Regulation. The CE marking should be the only marking which guarantees that products with digital elements comply with the requirements of this Regulation. 1. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).	elements should be laid down in this Regulation. The CE marking should be the only marking which guarantees that products with digital elements comply with the requirements of this Regulation. 1. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30). Text Origin: Commission Proposal

Recital 44

54	(44) In order to allow economic operators to demonstrate conformity with the essential requirements laid down in this Regulation and to allow market surveillance authorities to ensure that products with digital elements made available on the market comply with these requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council¹ establishes modules for conformity assessment procedures in proportion to the level of risk involved and the level of security required. In order to ensure inter-sectoral coherence and	(44) In order to allow economic operators to demonstrate conformity with the essential requirements laid down in this Regulation and to allow market surveillance authorities to ensure that products with digital elements made available on the market comply with these requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council¹ establishes modules for conformity assessment procedures in proportion to the level of risk involved and the level of security required. In order to ensure inter-sectoral coherence and	(44) In order to allow economic operators to demonstrate conformity with the essential requirements laid down in this Regulation and to allow market surveillance authorities to ensure that products with digital elements made available on the market comply with these requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council¹ establishes modules for conformity assessment procedures in proportion to the level of risk involved and the level of security required. In order to ensure inter-sectoral coherence and	(44) In order to allow economic operators to demonstrate conformity with the essential requirements laid down in this Regulation and to allow market surveillance authorities to ensure that products with digital elements made available on the market comply with these requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council¹ establishes modules for conformity assessment procedures in proportion to the level of risk involved and the level of security required. In order to ensure inter-sectoral coherence and

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	to avoid ad-hoc variants, conformity assessment procedures adequate for verifying the conformity of products with digital elements with the essential requirements set out in this Regulation have been based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole life cycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product. 1. Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).	to avoid ad-hoc variants, conformity assessment procedures adequate for verifying the conformity of products with digital elements with the essential requirements set out in this Regulation have been based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole life cycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product. 1. Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).	to avoid ad-hoc variants, conformity assessment procedures adequate for verifying the conformity of products with digital elements with the essential requirements set out in this Regulation have been based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole life cycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product. 1. Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).	to avoid ad-hoc variants, conformity assessment procedures adequate for verifying the conformity of products with digital elements with the essential requirements set out in this Regulation have been based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole life cycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product. 1. Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82). Text Origin: Commission Proposal
Recital 45				
55	(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	(45) As a general rule the conformity assessment of products with digital elements should be <u>risk-based and in most cases</u> 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	(45) ~~As a general rule the~~ Conformity assessment of products with digital elements ~~should~~that are not covered by Annex III or IIIa of this Regulation can be carried out by the manufacturer under its own responsibility following the internal control procedure based on Module A of Decision 768/2008/EC	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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~~ <i>manufacturer does not apply such those</i> harmonised standards, common specifications or cybersecurity certification schemes <u>have been in place for a minimum period of time enabling manufacturers to adopt them and the manufacturer does not apply them</u>, 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	as set out in Annex VI of this Regulation. This also applies to cases where a manufacturer should retain chooses to not apply in whole or in part an applicable harmonised standard, common specification or European cybersecurity certification. The manufacturer retains flexibility to choose a stricter conformity assessment procedure involving a third-party. ~~If~~ Under the internal control conformity assessment procedure, the manufacturer ensures and declares on its sole responsibility that the product is classified as a critical with digital elements meets all the essential requirements set out in Section 1 of Annex I of this Regulation and that the processes of the manufacturer meet the essential requirements set out in Section 2 of Annex I of this Regulation. If the product belongs to 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	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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.	responsibility (module A). If the manufacturer does not apply such harmonised standards, common specifications or European cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party (based on Modules B and C or H). Taking into account the administrative burden on manufacturers and the fact that cybersecurity plays an important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures respectively based on modules B+C or module H of Decision 768/2008/EC have been chosen as most appropriate for assessing the compliance of ~~critical~~ products with digital elements belonging to a category referred to in Annex III, in a proportionate and effective manner. The manufacturer that carries out the third-party conformity assessment can choose the procedure that suits best its design and production process. Given the even greater cybersecurity risk linked with the use of ~~products classified as critical~~ class II products, the conformity assessment should always involve a third party, even where the product complies fully or partly with harmonised standards, common specifications or European cybersecurity	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			certification.	
Recital 46				
56	(46) While the creation of tangible products with digital elements usually requires manufacturers to make substantial efforts throughout the design, development and production phases, the creation of products with digital elements in the form of software almost exclusively focuses on design and development, while the production phase plays a minor role. Nonetheless, in many cases software products still need to be compiled, built, packaged, made available for download or copied onto physical media before being placed on the market. These activities should be considered as activities amounting to production when applying the relevant conformity assessment modules to verify the compliance of the product with the essential requirements of this Regulation across the design, development and production phases.	(46) While the creation of tangible products with digital elements usually requires manufacturers to make substantial efforts throughout the design, development and production phases, the creation of products with digital elements in the form of software almost exclusively focuses on design and development, while the production phase plays a minor role. Nonetheless, in many cases software products still need to be compiled, built, packaged, made available for download or copied onto physical media before being placed on the market. These activities should be considered as activities amounting to production when applying the relevant conformity assessment modules to verify the compliance of the product with the essential requirements of this Regulation across the design, development and production phases.	(46) While the creation of tangible products with digital elements usually requires manufacturers to make substantial efforts throughout the design, development and production phases, the creation of products with digital elements in the form of software almost exclusively focuses on design and development, while the production phase plays a minor role. Nonetheless, in many cases software products still need to be compiled, built, packaged, made available for download or copied onto physical media before being placed on the market. These activities should be considered as activities amounting to production when applying the relevant conformity assessment modules to verify the compliance of the product with the essential requirements of this Regulation across the design, development and production phases.	(46) While the creation of tangible products with digital elements usually requires manufacturers to make substantial efforts throughout the design, development and production phases, the creation of products with digital elements in the form of software almost exclusively focuses on design and development, while the production phase plays a minor role. Nonetheless, in many cases software products still need to be compiled, built, packaged, made available for download or copied onto physical media before being placed on the market. These activities should be considered as activities amounting to production when applying the relevant conformity assessment modules to verify the compliance of the product with the essential requirements of this Regulation across the design, development and production phases. Text Origin: Commission Proposal
Recital 46a				
56a			(46a) In relation to small and	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			micro enterprises, in order to ensure proportionality, it is appropriate to alleviate administrative costs without affecting the level of cybersecurity protection of products with digital elements under the scope of this Regulation or the level playing field among manufacturers. Therefore, it is appropriate for the Commission to establish a simplified technical documentation form targeted at the needs of small and micro enterprises.	
Recital 46b				
56b			(46b) In order to promote and protect innovation, it is important that the interests of SME manufactures, in particular small and micro enterprises, including start-ups, are taken into particular account. To this objective, Member States could develop initiatives which are targeted at small and micro manufacturers, including on training, awareness raising, information communication and on testing and third-party conformity assessment activities. Translation costs related to mandatory documentation, such as the technical documentation and the information and	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			instructions for the user as required by this Regulation, and communication with authorities may constitute a significant cost for manufacturers, notably those of a smaller scale. Therefore, Member States may consider that one of the languages determined and accepted by them for relevant manufacturers' documentation and for communication with manufacturer is one which is broadly understood by the largest possible number of users.	
Recital 46c				
56c			(46c) In order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market, as well as in order to facilitate compliance of manufacturers, notably small and micro enterprises, with their obligations laid down in this Regulation, relevant EU funding programmes, as well as the European Cybersecurity Competence Center and National Coordination Centres and the European Digital Innovation Hubs established by the Commission and the Member States at national or EU level may contribute to the implementation of this Regulation. Within their respective mission	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			and fields of competence, they may provide technical and scientific support to small and micro manufacturers, such as for testing activities and third-party conformity assessment. They can also foster the deployment of tools to facilitate the implementation of this Regulation.	
Recital 46d				
56d			(46d) Considering the costs that third-party conformity assessment may entail, funding initiatives at Union level that seek to alleviate such costs for micro and small enterprises should be considered.	
Recital 46e				
56e			(46e) The Commission should actively support the Member States and economic operators in the implementation and enforcement of this Regulation. Guidance and standardised templates can reduce costs related to familiarisation with this Regulation and related to legal uncertainty especially for smaller companies. Such documents should be developed on particular topics aiming at facilitating the application of this Regulation,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			while paying particular attention to the needs of small and micro enterprises. The Commission should facilitate the development of such documents and ensure the consultation of relevant stakeholders. Similarly, market surveillance authorities may also consider providing guidance and advice to economic operators on the implementation of the Regulation, paying particular attention to micro and small enterprises. In doing so, they should coordinate as appropriate through the ADCO to ensure a consistent implementation of this Regulation.	
Recital 46f				
56f			(46f) Micro, small and medium-sized enterprises or ‘SMEs’ referred to in this Regulation mean micro, small and medium-sized enterprises as defined in the Annex to Recommendation 2003/361/EC. When determining the category an enterprise falls into, the provisions of that Annex should be applied in their entirety. Therefore, when calculating the staff headcount and financial ceilings determining the enterprise categories, the provisions of Article 6 of the Annex to	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			Recommendation 2003/361/EC on establishing the data of an enterprise in consideration of specific types of enterprises, such as partner enterprises or linked enterprises, should also apply.	
Recital 47				
57	(47) In order to carry out third-party conformity assessment for products with digital elements, conformity assessment bodies should be notified by the national notifying authorities to the Commission and the other Member States, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.	(47) In order to carry out third-party conformity assessment for products with digital elements, conformity assessment bodies should be notified by the national notifying authorities to the Commission and the other Member States, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.	(47) In order to carry out third-party conformity assessment for products with digital elements, conformity assessment bodies should be notified by the national notifying authorities to the Commission and the other Member States, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.	(47) In order to carry out third-party conformity assessment for products with digital elements, conformity assessment bodies should be notified by the national notifying authorities to the Commission and the other Member States, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests. Text Origin: Commission Proposal
Recital 48				
58	(48) In order to ensure a consistent level of quality in the performance of conformity assessment of products with digital elements, it is also necessary to lay down requirements for notifying authorities and other bodies involved in the assessment, notification and monitoring of notified bodies. The	(48) In order to ensure a consistent level of quality in the performance of conformity assessment of products with digital elements, it is also necessary to lay down requirements for notifying authorities and other bodies involved in the assessment, notification and monitoring of notified bodies. The	(48) In order to ensure a consistent level of quality in the performance of conformity assessment of products with digital elements, it is also necessary to lay down requirements for notifying authorities and other bodies involved in the assessment, notification and monitoring of notified bodies. The	(48) In order to ensure a consistent level of quality in the performance of conformity assessment of products with digital elements, it is also necessary to lay down requirements for notifying authorities and other bodies involved in the assessment, notification and monitoring of notified bodies. The

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008. Since accreditation is an essential means of verifying the competence of conformity assessment bodies, it should also be used for the purposes of notification.	system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008. Since accreditation is an essential means of verifying the competence of conformity assessment bodies, it should also be used for the purposes of notification.	system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008. Since accreditation is an essential means of verifying the competence of conformity assessment bodies, it should also be used for the purposes of notification.	system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008. Since accreditation is an essential means of verifying the competence of conformity assessment bodies, it should also be used for the purposes of notification. Text Origin: Commission Proposal
Recital 48a				
58a			(48a) Conformity assessment bodies that have been accredited and notified under Union legislation laying down similar requirements, such as a conformity assessment body that has been notified for a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 or notified under the Delegated Regulation (EU) 2022/30, should be newly assessed and notified under this Regulation. However, synergies can be defined by relevant authorities regarding any overlapping requirements in order to prevent an unnecessary financial and administrative burden and ensure a smooth and timely notification process.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 49				
59	(49) Transparent accreditation as provided for in Regulation (EC) No 765/2008, ensuring the necessary level of confidence in certificates of conformity, should be considered by the national public authorities throughout the Union as the preferred means of demonstrating the technical competence of conformity assessment bodies. However, national authorities may consider that they possess the appropriate means of carrying out that evaluation themselves. In such cases, in order to ensure the appropriate level of credibility of evaluations carried out by other national authorities, they should provide the Commission and the other Member States with the necessary documentary evidence demonstrating the compliance of the conformity assessment bodies evaluated with the relevant regulatory requirements.	(49) Transparent accreditation as provided for in Regulation (EC) No 765/2008, ensuring the necessary level of confidence in certificates of conformity, should be considered by the national public authorities throughout the Union as the preferred means of demonstrating the technical competence of conformity assessment bodies. However, national authorities may consider that they possess the appropriate means of carrying out that evaluation themselves. In such cases, in order to ensure the appropriate level of credibility of evaluations carried out by other national authorities, they should provide the Commission and the other Member States with the necessary documentary evidence demonstrating the compliance of the conformity assessment bodies evaluated with the relevant regulatory requirements.	(49) Transparent accreditation as provided for in Regulation (EC) No 765/2008, ensuring the necessary level of confidence in certificates of conformity, should be considered by the national public authorities throughout the Union as the preferred means of demonstrating the technical competence of conformity assessment bodies. However, national authorities may consider that they possess the appropriate means of carrying out that evaluation themselves. In such cases, in order to ensure the appropriate level of credibility of evaluations carried out by other national authorities, they should provide the Commission and the other Member States with the necessary documentary evidence demonstrating the compliance of the conformity assessment bodies evaluated with the relevant regulatory requirements.	(49) Transparent accreditation as provided for in Regulation (EC) No 765/2008, ensuring the necessary level of confidence in certificates of conformity, should be considered by the national public authorities throughout the Union as the preferred means of demonstrating the technical competence of conformity assessment bodies. However, national authorities may consider that they possess the appropriate means of carrying out that evaluation themselves. In such cases, in order to ensure the appropriate level of credibility of evaluations carried out by other national authorities, they should provide the Commission and the other Member States with the necessary documentary evidence demonstrating the compliance of the conformity assessment bodies evaluated with the relevant regulatory requirements. Text Origin: Commission Proposal
Recital 50				
60	(50) Conformity assessment bodies	(50) Conformity assessment bodies	(50) Conformity assessment bodies	(50) Conformity assessment bodies

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	frequently subcontract parts of their activities linked to the assessment of conformity or have recourse to a subsidiary. In order to safeguard the level of protection required for the product with digital elements to be placed on the market, it is essential that conformity assessment subcontractors and subsidiaries fulfil the same requirements as notified bodies in relation to the performance of conformity assessment tasks.	frequently subcontract parts of their activities linked to the assessment of conformity or have recourse to a subsidiary. In order to safeguard the level of protection required for the product with digital elements to be placed on the market, it is essential that conformity assessment subcontractors and subsidiaries fulfil the same requirements as notified bodies in relation to the performance of conformity assessment tasks.	frequently subcontract parts of their activities linked to the assessment of conformity or have recourse to a subsidiary. In order to safeguard the level of protection required for the product with digital elements to be placed on the market, it is essential that conformity assessment subcontractors and subsidiaries fulfil the same requirements as notified bodies in relation to the performance of conformity assessment tasks.	frequently subcontract parts of their activities linked to the assessment of conformity or have recourse to a subsidiary. In order to safeguard the level of protection required for the product with digital elements to be placed on the market, it is essential that conformity assessment subcontractors and subsidiaries fulfil the same requirements as notified bodies in relation to the performance of conformity assessment tasks. Text Origin: Commission Proposal
Recital 51				
61	(51) The notification of a conformity assessment body should be sent by the notifying authority to the Commission and the other Member States via the New Approach Notified and Designated Organisations (NANDO) information system. NANDO is the electronic notification tool developed and managed by the Commission where a list of all notified bodies can be found.	(51) The notification of a conformity assessment body should be sent by the notifying authority to the Commission and the other Member States via the New Approach Notified and Designated Organisations (NANDO) information system. NANDO is the electronic notification tool developed and managed by the Commission where a list of all notified bodies can be found.	(51) The notification of a conformity assessment body should be sent by the notifying authority to the Commission and the other Member States via the New Approach Notified and Designated Organisations (NANDO) information system. NANDO is the electronic notification tool developed and managed by the Commission where a list of all notified bodies can be found.	(51) The notification of a conformity assessment body should be sent by the notifying authority to the Commission and the other Member States via the New Approach Notified and Designated Organisations (NANDO) information system. NANDO is the electronic notification tool developed and managed by the Commission where a list of all notified bodies can be found. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 52				
62	(52) Since notified bodies may offer their services throughout the Union, it is appropriate to give the other Member States and the Commission the opportunity to raise objections concerning a notified body. It is therefore important to provide for a period during which any doubts or concerns as to the competence of conformity assessment bodies can be clarified before they start operating as notified bodies.	(52) Since notified bodies may offer their services throughout the Union, it is appropriate to give the other Member States and the Commission the opportunity to raise objections concerning a notified body. It is therefore important to provide for a period during which any doubts or concerns as to the competence of conformity assessment bodies can be clarified before they start operating as notified bodies.	(52) Since notified bodies may offer their services throughout the Union, it is appropriate to give the other Member States and the Commission the opportunity to raise objections concerning a notified body. It is therefore important to provide for a period during which any doubts or concerns as to the competence of conformity assessment bodies can be clarified before they start operating as notified bodies.	(52) Since notified bodies may offer their services throughout the Union, it is appropriate to give the other Member States and the Commission the opportunity to raise objections concerning a notified body. It is therefore important to provide for a period during which any doubts or concerns as to the competence of conformity assessment bodies can be clarified before they start operating as notified bodies. Text Origin: Commission Proposal
Recital 53				
63	(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.	(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators, <u>in particular for microenterprises and small and medium-sized enterprises. In this regard, Member States, with the support of the Commission, should ensure that there is an adequate availability of skilled professionals in order to ensure that notified bodies can carry out their activities efficiently, thus minimising possible impediments, avoiding bottlenecks</u>	(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement	
		<i><u>and facilitating economic operators' compliance with this Regulation.</u></i> For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.	PUBLIC		
Recital 53a					
63a		<i><u>(53a) In order to increase efficiency and transparency, Member States should ensure, before the date of application of this Regulation, that there is a sufficient number of notified bodies in the Union to carry out conformity assessments. The Commission should monitor market developments and assist Member States in this endeavour, in order to avoid bottlenecks and hindrances to market entry.</u></i>			
Recital 54					
64	(54) Market surveillance is an essential instrument in ensuring the proper and uniform application of Union legislation. It is therefore appropriate to put in place a legal	(54) Market surveillance is an essential instrument in ensuring the proper and uniform application of Union legislation. It is therefore appropriate to put in place a legal	(54) Market surveillance is an essential instrument in ensuring the proper and uniform application of Union legislation. It is therefore appropriate to put in place a legal	(54) Market surveillance is an essential instrument in ensuring the proper and uniform application of Union legislation. It is therefore appropriate to put in place a legal	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	framework within which market surveillance can be carried out in an appropriate manner. Rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 of the European Parliament and of the Council¹ apply to products with digital elements covered by this Regulation. 1. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).	framework within which market surveillance can be carried out in an appropriate manner. Rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 of the European Parliament and of the Council¹ apply to products with digital elements covered by this Regulation. 1. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).	framework within which market surveillance can be carried out in an appropriate manner. Rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 of the European Parliament and of the Council¹ apply to products with digital elements covered by this Regulation. 1. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).	framework within which market surveillance can be carried out in an appropriate manner. Rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 of the European Parliament and of the Council¹ apply to products with digital elements covered by this Regulation. 1. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1). Text Origin: Commission Proposal

Recital 55

65	(55) In accordance with Regulation (EU) 2019/1020, market surveillance authorities carry out market surveillance in the territory of that Member State. This Regulation should not prevent Member States from choosing the competent authorities to carry out those tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States may choose to designate any existing or new authority to act as market surveillance authority,	(55) In accordance with Regulation (EU) 2019/1020, market surveillance authorities carry out market surveillance in the territory of that Member State. This Regulation should not prevent Member States from choosing the competent authorities to carry out those tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States may choose to designate any existing or new authority to act as market surveillance authority,	(55) In accordance with Regulation (EU) 2019/1020, market surveillance authorities carry out market surveillance in the territory of that Member State. This Regulation should not prevent Member States from choosing the competent authorities to carry out those tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States may choose to designate any existing or new authority to act as market surveillance authority,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	including national competent authorities referred to in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] or designated national cybersecurity certification authorities referred to in Article 58 of Regulation (EU) 2019/881. Economic operators should fully cooperate with market surveillance authorities and other competent authorities. Each Member State should inform the Commission and the other Member States of its market surveillance authorities and the areas of competence of each of those authorities and should ensure the necessary resources and skills to carry out the surveillance tasks relating to this Regulation. As per Article 10(2) and (3) of Regulation (EU) 2019/1020, each Member State should appoint a single liaison office that should be responsible, among others, for representing the coordinated position of the market surveillance authorities and assisting in the cooperation between market surveillance authorities in different Member States.	including national competent authorities referred to in ~~Article [Article X] of Directive [Directive XXX/XXXX (NIS2EU)]~~ 2022/2555 or designated national cybersecurity certification authorities referred to in Article 58 of Regulation (EU) 2019/881. Economic operators should fully cooperate with market surveillance authorities and other competent authorities. Each Member State should inform the Commission and the other Member States of its market surveillance authorities and the areas of competence of each of those authorities and should ensure the necessary resources and skills to carry out the surveillance tasks relating to this Regulation. As per Article 10(2) and (3) of Regulation (EU) 2019/1020, each Member State should appoint a single liaison office that should be responsible, among others, for representing the coordinated position of the market surveillance authorities and assisting in the cooperation between market surveillance authorities in different Member States.	including ~~national~~ competent authorities established pursuant to ~~referred to in Article [Article X] 8 of Directive [Directive XXX/XXXX (NIS2EU)]~~ 2022/2555 or designated national cybersecurity certification authorities referred to in Article 58 of Regulation (EU) 2019/881 or market surveillance authorities designated for the purpose of Directive 2014/53/EU. Economic operators should fully cooperate with market surveillance authorities and other competent authorities. Each Member State should inform the Commission and the other Member States of its market surveillance authorities and the areas of competence of each of those authorities and should ensure the necessary resources and skills to carry out the surveillance tasks relating to this Regulation. As per Article 10(2) and (3) of Regulation (EU) 2019/1020, each Member State should appoint a single liaison office that should be responsible, among others, for representing the coordinated position of the market surveillance authorities and assisting in the cooperation between market surveillance authorities in different Member States.	

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

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			as the one established under Directive 2014/53/EU.	
Recital 56a				
66a			(56a) Market surveillance authorities, through the ADCO established under this Regulation, should cooperate closely and should be able to develop guidance documents to facilitate market surveillance activities at national level, such as by developing best practices and indicators to effectively check the compliance of products with digital elements.	
Recital 57				
67	(57) In order to ensure timely, proportionate and effective measures in relation to products with digital elements presenting a significant cybersecurity risk, a Union safeguard procedure should be foreseen under which interested parties are informed of measures intended to be taken with regard to such products. This should also allow market surveillance authorities, in cooperation with the relevant economic operators, to act at an earlier stage where necessary. Where the Member States and the Commission agree as to the	(57) In order to ensure timely, proportionate and effective measures in relation to products with digital elements presenting a significant cybersecurity risk, a Union safeguard procedure should be ~~foreseen~~ <u>provided</u> under which interested parties are informed of measures intended to be taken with regard to such products. This should also allow market surveillance authorities, in cooperation with the relevant economic operators, to act at an earlier stage where necessary. Where the Member States and the Commission agree as to the	(57) In order to ensure timely, proportionate and effective measures in relation to products with digital elements presenting a significant cybersecurity risk, a Union safeguard procedure should be foreseen under which interested parties are informed of measures intended to be taken with regard to such products. This should also allow market surveillance authorities, in cooperation with the relevant economic operators, to act at an earlier stage where necessary. Where the Member States and the Commission agree as to the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	justification of a measure taken by a Member State, no further involvement of the Commission should be required, except where non-compliance can be attributed to shortcomings of a harmonised standard.	justification of a measure taken by a Member State, no further involvement of the Commission should be required, except where non-compliance can be attributed to shortcomings of a harmonised standard.	justification of a measure taken by a Member State, no further involvement of the Commission should be required, except where non-compliance can be attributed to shortcomings of a harmonised standard.	
Recital 58				
68	(58) In certain cases, a product with digital elements which complies with this Regulation, may nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in [Annex I to Directive XXX/XXXX (NIS2)] or to other aspects of public interest protection. Therefore it is necessary to establish rules which ensure mitigation of those risks. As a result, market surveillance authorities should take measures to require the economic operator to ensure that the product no longer presents that risk, to recall it or to withdraw it, depending on the risk. As soon as a market surveillance authority	(58) In certain cases, a product with digital elements which complies with this Regulation, may nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in ~~[Annex I to Directive XXX/XXXX (NIS2EU)]~~ 2022/2555 or to other aspects of public interest protection. Therefore it is necessary to establish rules which ensure mitigation of those risks. As a result, market surveillance authorities should take measures to require the economic operator to ensure that the product no longer presents that risk, to recall it or to withdraw it, depending on the risk. As soon as a market	(58) In certain cases, a product with digital elements which complies with this Regulation, may nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by ~~essential~~ entities of the type referred to in [Annex I to Directive XXX/XXXX (NIS2EU)] 2022/2555 or to other aspects of public interest protection. Therefore it is necessary to establish rules which ensure mitigation of those risks. As a result, market surveillance authorities should take measures to require the economic operator to ensure that the product no longer presents that risk, to recall it or to withdraw it, depending on the risk. As soon as a market	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	restricts or forbids the free movement of a product in such way, the Member State should notify without delay the Commission and the other Member States of the provisional measures, indicating the reasons and justification for the decision. Where a market surveillance authority adopts such measures against products presenting a risk, the Commission should enter into consultation with the Member States and the relevant economic operator or operators without delay and should evaluate the national measure. On the basis of the results of this evaluation, the Commission should decide whether the national measure is justified or not. The Commission should address its decision to all Member States and immediately communicate it to them and the relevant economic operator or operators. If the measure is considered justified, the Commission may also consider adopting proposals to revise the respective Union legislation.	surveillance authority restricts or forbids the free movement of a product in such way, the Member State should notify without delay the Commission and the other Member States of the provisional measures, indicating the reasons and justification for the decision. Where a market surveillance authority adopts such measures against products presenting a risk, the Commission should enter into consultation with the Member States and the relevant economic operator or operators without delay and should evaluate the national measure. On the basis of the results of this evaluation, the Commission should decide whether the national measure is justified or not. The Commission should address its decision to all Member States and immediately communicate it to them and the relevant economic operator or operators. If the measure is considered justified, the Commission may also consider adopting proposals to revise the respective Union legislation.	surveillance authority restricts or forbids the free movement of a product in such way, the Member State should notify without delay the Commission and the other Member States of the provisional measures, indicating the reasons and justification for the decision. Where a market surveillance authority adopts such measures against products presenting a risk, the Commission should enter into consultation with the Member States and the relevant economic operator or operators without delay and should evaluate the national measure. On the basis of the results of this evaluation, the Commission should decide whether the national measure is justified or not. The Commission should address its decision to all Member States and immediately communicate it to them and the relevant economic operator or operators. If the measure is considered justified, the Commission may also consider adopting proposals to revise the respective Union legislation.	
Recital 59				
69	(59) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that these are not	(59) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that these are not	(59) For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that these are not	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	compliant with this Regulation, or for products that are compliant with this Regulation, but that present other important risks, such as risks to the health or safety of persons, fundamental rights or the provision of the services by essential entities of the type referred to in [Annex I of Directive XXX / XXXX (NIS2)], the Commission may request ENISA to carry out an evaluation. Based on that evaluation, the Commission may adopt, through implementing acts, corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling of the respective products, within a reasonable period, commensurate with the nature of the risk. The Commission may have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the good functioning of the internal market, and only where no effective measures have been taken by surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities under the scope of [Directive XXX / XXXX (NIS2)], while containing known vulnerabilities that are being	compliant with this Regulation, or for products that are compliant with this Regulation, but that present other important risks, such as risks to the health or safety of persons, fundamental rights or the provision of the services by essential entities of the type referred to in ~~[Annex I of Directive XXX / XXXX (NIS2EU)]~~ <u>2022/2555</u>, the Commission may request ENISA to carry out an evaluation. Based on that evaluation, the Commission may adopt, through implementing acts, corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling of the respective products, within a reasonable period, commensurate with the nature of the risk. The Commission may have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the good functioning of the internal market, and only where no effective measures have been taken by surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities ~~under that fall within~~ the scope of ~~[Directive XXX / XXXX (NIS2EU)]~~	compliant with this Regulation, or for products that are compliant with this Regulation, but that present other important risks, such as risks to the health or safety of persons, fundamental rights or the provision of the services by ~~essential~~ entities of ~~the~~ type referred to in ~~[Annex I of Directive XXX / XXXX (NIS2EU)]~~ <u>2022/2555</u>, the Commission may request ENISA to carry out an evaluation. Based on that evaluation, the Commission may adopt, through implementing acts, corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling of the respective products, within a reasonable period, commensurate with the nature of the risk. The Commission may have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the good functioning of the internal market, and only where no effective measures have been taken by surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities under the scope of ~~[Directive XXX / XXXX (NIS2EU)]~~ <u>2022/2555</u>, while	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the non-compliance with this Regulation or the important risks presented persist.	2022/2555 , while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the non-compliance with this Regulation or the important risks presented persist.	containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the non-compliance with this Regulation or the important risks presented persist.	
Recital 60				
70	(60) In cases where there are indications of non-compliance with this Regulation in several Member States, market surveillance authorities should be able to carry out joint activities with other authorities, with a view to verifying compliance and identifying cybersecurity risks of products with digital elements.	(60) In cases where there are indications of non-compliance with this Regulation in several Member States, market surveillance authorities should be able to carry out joint activities with other authorities, with a view to verifying compliance and identifying cybersecurity risks of products with digital elements.	(60) In cases where there are indications of non-compliance with this Regulation in several Member States, market surveillance authorities should be able to carry out joint activities with other authorities, with a view to verifying compliance and identifying cybersecurity risks of products with digital elements.	(60) In cases where there are indications of non-compliance with this Regulation in several Member States, market surveillance authorities should be able to carry out joint activities with other authorities, with a view to verifying compliance and identifying cybersecurity risks of products with digital elements. Text Origin: Commission Proposal
Recital 61				
71	(61) Simultaneous coordinated control actions ('sweeps') are specific enforcement actions by market surveillance authorities that can further enhance product security.	(61) Simultaneous coordinated control actions ('sweeps') are specific enforcement actions by market surveillance authorities that can further enhance product security.	(61) Simultaneous coordinated control actions ('sweeps') are specific enforcement actions by market surveillance authorities that can further enhance product security.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps could be organised to the market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives.	Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps ~~could~~ <u>should</u> be organised to the market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives. <u><i>The Commission should also coordinate market surveillance authorities in the regular inspections of products with digital elements that might present a security risk for the Union, including in light of the non-technical risk factor.</i></u>	Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps could be organised to the market surveillance authorities, based, among others, on the ~~notifications of product~~ information it receives in relation to vulnerabilities and incidents it receives.	
Recital 62				
72	(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	(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	(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~~ on the Functioning of the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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 criteria 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-Making¹. 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	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 <u>specifying 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 of this Regulation</u>, the potential mandating of certification of certain highly critical products with digital elements based on criticality criteria 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. <u>Powers to adopt delegated acts should also be delegated to the Commission to specify the format and elements of the software bill of materials, specify further the format and procedure of the notifications on actively exploited vulnerabilities and significant incidents submitted</u>	European Union 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 in respect of updates to the lists of categories of products with digital elements in Annexes III and IIIa .- 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 criteria set out in this Regulation and an impact assessment, 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~~ Interinstitutional Agreement of 13 April 2016 on	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. 1. OJ L 123, 12.5.2016, p. 1.	<u>to ENISA by the manufacturers. Where necessary, the Commission should be empowered to adopt delegated acts to adopt common specifications in respect of the essential requirements set out in Annex I.</u> 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-Making¹. 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. <u>For the purpose of developing delegated acts pursuant to this Regulation, the Commission should consult the cyber resilience Expert Group. The Commission should also conduct regular structural dialogue with economic operators and carry out public consultations, inter alia for the purposes of evaluating the scope of this Regulation and whether certain categories of</u>	Better Law-Making¹. 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. 1. OJ L 123, 12.5.2016, p. 1.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>products should be included or excluded.</u> 1. OJ L 123, 12.5.2016, p. 1.		
Recital 63				
73	(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	(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~~ <u>lay down technical specifications for labelling</u> 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, including~~ <u>harmonised labels</u>, ~~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,	(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to: specify the definitions of the categories of products with digital elements listed in Annexes III and IIIa, specify the format and elements of the software bill of materials and the format of the information and instructions referred to in Annex II, specify further the type of information, format and procedure of the notifications on actively exploited vulnerabilities and incidents ~~submitted to ENISA~~ having an impact on the security of products with digital elements submitted by the manufacturers, establish common specifications covering technical requirements that provide a means to comply with the essential requirements set out in Annex I, specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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 Council¹. ¹. 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).	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 Council¹. ¹. 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~~ 13).	demonstrate conformity with the essential requirements or parts ~~thereof~~ as set out in Annex I ~~to this Regulation~~, ~~adopt common specifications in respect of the essential requirements set out in Annex I and related conformity assessment procedures~~, 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 Council¹. ¹. 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).	
Recital 64				
74	(64) In order to ensure trustful and constructive cooperation of market surveillance authorities at Union and	(64) In order to ensure trustful and constructive cooperation of market surveillance authorities at Union and	(64) In order to ensure trustful and constructive cooperation of market surveillance authorities at Union and	(64) In order to ensure trustful and constructive cooperation of market surveillance authorities at Union and

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.	national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.	national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.	national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks. Text Origin: Commission Proposal
Recital 65				
75	(65) In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. Maximum levels for administrative fines to be provided for in national laws for non-compliance with the obligations laid down in this Regulation should therefore be established. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation should be taken into account and as a minimum those explicitly established in this Regulation, including whether administrative fines have been already applied by other market surveillance authorities to the same operator for similar infringements. Such circumstances can be either	(65) In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. Maximum levels for administrative fines to be provided for in national laws for non-compliance with the obligations laid down in this Regulation should therefore be established. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation should be taken into account and as a minimum those explicitly established in this Regulation, including whether <u>the manufacturer is a microenterprise, a small or medium-sized enterprise or a start-up and</u> administrative fines have been already applied by other market surveillance authorities	(65) In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. Maximum levels for administrative fines to be provided for in national laws for non-compliance with the obligations laid down in this Regulation should therefore be established. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation should be taken into account and as a minimum those explicitly established in this Regulation, including whether administrative fines have been already applied by other market surveillance authorities to the same operator for similar infringements. Such circumstances can be either	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	aggravating, in situations where the infringement by the same operator persists on the territory of other Member States than the one where an administrative fine has already been applied, or mitigating, in ensuring that any other administrative fine considered by another market surveillance authority for the same economic operator or the same type of breach should already take account, along with other relevant specific circumstances, of a penalty and the quantum thereof imposed in other Member States. In all such cases, the cumulative administrative fine that could be applied by market surveillance authorities of several Member States to the same economic operator for the same type of infringement should ensure the respect of the principle of proportionality.	to the same operator for similar infringements. Such circumstances can be either aggravating, in situations where the infringement by the same operator persists on the territory of other Member States than the one where an administrative fine has already been applied, or mitigating, in ensuring that any other administrative fine considered by another market surveillance authority for the same economic operator or the same type of breach should already take account, along with other relevant specific circumstances, of a penalty and the quantum thereof imposed in other Member States. In all such cases, the cumulative administrative fine that could be applied by market surveillance authorities of several Member States to the same economic operator for the same type of infringement should ensure the respect of the principle of proportionality.	aggravating, in situations where the infringement by the same operator persists on the territory of other Member States than the one where an administrative fine has already been applied, or mitigating, in ensuring that any other administrative fine considered by another market surveillance authority for the same economic operator or the same type of breach should already take account, along with other relevant specific circumstances, of a penalty and the quantum thereof imposed in other Member States. In all such cases, the cumulative administrative fine that could be applied by market surveillance authorities of several Member States to the same economic operator for the same type of infringement should ensure the respect of the principle of proportionality.	
Recital 66				
76	(66) Where administrative fines are imposed on persons that are not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the	(66) Where administrative fines are imposed on persons that are not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the	(66) Where administrative fines are imposed on persons that are not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the	(66) Where administrative fines are imposed on persons that are not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines.	appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines.	appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines.	appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Text Origin: Commission Proposal
Recital 66a				
76a		<u>(66a) The revenues generated from the payments of penalties should be used to strengthen the level of cybersecurity within the Union, including by developing capacity and skills related to cybersecurity, improving economic operators' cyber resilience, in particular of microenterprises and of small and medium-sized enterprises and more in general fostering public awareness of cyber security issues.</u>		
Recital 67				
77	(67) In its relationships with third countries, the EU endeavours to promote international trade in regulated products. A broad variety of measures can be applied in order to facilitate trade, including several legal instruments such as bilateral (inter-governmental) Mutual Recognition Agreements (MRAs)	(67) In its relationships with third countries, the EU endeavours to promote international trade in regulated products. A broad variety of measures can be applied in order to facilitate trade, including several legal instruments such as bilateral (inter-governmental) Mutual Recognition Agreements (MRAs)	(67) In its relationships with third countries, the EU endeavours to promote international trade in regulated products. A broad variety of measures can be applied in order to facilitate trade, including several legal instruments such as bilateral (inter-governmental) Mutual Recognition Agreements (MRAs)	(67) In its relationships with third countries, the EU endeavours to promote international trade in regulated products. A broad variety of measures can be applied in order to facilitate trade, including several legal instruments such as bilateral (inter-governmental) Mutual Recognition Agreements (MRAs)

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	for conformity assessment and marking of regulated products. MRAs are established between the Union and third countries, which are on a comparable level of technical development and have a compatible approach concerning conformity assessment. These agreements are based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party. Currently MRAs are in place for several countries. The agreements are concluded in a number of specific sectors, which might vary from one country to another. In order to further facilitate trade, and recognising that supply chains of products with digital elements are global, MRAs concerning conformity assessment may be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU. Cooperation with partner countries is also important, in order to strengthen cyber resilience globally, as in the long term this will contribute to a strengthened cybersecurity framework both within and outside of the EU.	for conformity assessment and marking of regulated products. MRAs are established between the Union and third countries, which are on a comparable level of technical development and have a compatible approach concerning conformity assessment. These agreements are based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party. Currently MRAs are in place for several countries. The agreements are concluded in a number of specific sectors, which might vary from one country to another. In order to further facilitate trade, and recognising that supply chains of products with digital elements are global, MRAs concerning conformity assessment may be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU. Cooperation with partner countries is also important, in order to strengthen cyber resilience globally, as in the long term this will contribute to a strengthened cybersecurity framework both within and outside of the EU.	for conformity assessment and marking of regulated products. MRAs are established between the Union and third countries, which are on a comparable level of technical development and have a compatible approach concerning conformity assessment. These agreements are based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party. Currently MRAs are in place for several countries. The agreements are concluded in a number of specific sectors, which might vary from one country to another. In order to further facilitate trade, and recognising that supply chains of products with digital elements are global, MRAs concerning conformity assessment may be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU. Cooperation with partner countries is also important, in order to strengthen cyber resilience globally, as in the long term this will contribute to a strengthened cybersecurity framework both within and outside of the EU.	for conformity assessment and marking of regulated products. MRAs are established between the Union and third countries, which are on a comparable level of technical development and have a compatible approach concerning conformity assessment. These agreements are based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party. Currently MRAs are in place for several countries. The agreements are concluded in a number of specific sectors, which might vary from one country to another. In order to further facilitate trade, and recognising that supply chains of products with digital elements are global, MRAs concerning conformity assessment may be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU. Cooperation with partner countries is also important, in order to strengthen cyber resilience globally, as in the long term this will contribute to a strengthened cybersecurity framework both within and outside of the EU. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 67a				
77a			(67a) Consumers should be entitled to enforce their rights in relation to the obligations imposed on economic operators under this Regulation through representative actions in accordance with Directive (EU) 2020/1828 of the European Parliament and of the Council¹. For that purpose, this Regulation should provide that Directive (EU) 2020/1828 is applicable to the representative actions concerning infringements of this Regulation that harm or can harm the collective interests of consumers. Annex I to that Directive should therefore be amended accordingly. It is for the Member States to ensure that that amendment is reflected in their transposition measures adopted in accordance with that Directive, although the adoption of national transposition measures in that regard is not a condition for the applicability of that Directive to those representative actions. The applicability of that Directive to the representative actions brought against infringements by economic operators of provisions of this Regulation that harm or can harm the collective interests of consumers should start from the date of application of this	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			Regulation. 1. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).	
Recital 68				
78	(68) The Commission should periodically review this Regulation, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.	(68) The Commission should periodically review this Regulation, in consultation with <u>the Expert Group and other</u> interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.	(68) The Commission should periodically review this Regulation, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.	
Recital 69				
79	(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 [~~24~~ ³⁶ months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [~~12~~ ¹⁸ 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 [~~24~~ ³⁶ months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents having an impact on the security of products with digital elements , which should apply [~~12~~ ²⁴ months] from the entry into force of	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			this Regulation.	
Recital 69a				
79a		<u>(69a) This Regulation will generate additional costs for microenterprises and small and medium-sized enterprises, including start-ups. In order to support these enterprises, the Commission should establish financial and technical support that enable these enterprises to contribute to the growth of the European economy and the European cybersecurity landscape, including by streamlining the financial support from the Digital Europe Programme and other relevant Union programmes as well as supporting companies and public sector organisations through European Digital Innovation Hubs. Furthermore, Member States should consider all possible complementary actions aiming to providing guidance and support for microenterprises and for small and medium-sized enterprises, including via the establishment of regulatory sandboxes, cybersecurity hubs and start-up accelerators.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Recital 70				
80	(70) Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	(70) Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	(70) Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	(70) Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective. Text Origin: Commission Proposal
Recital 71				
81	(71) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ¹ and delivered its opinion on [...], ¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision	(71) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ¹ and delivered its opinion on ~~...~~ ^{9 November 2022²} . ¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision	(71) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ¹ and delivered ~~its~~ ^{an} opinion on ~~...~~ ^{9 November 2022²} , ¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).	No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39). 2. OJ C 452, 29.11.2022, p. 23.	No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39). 2. OJ C 452, 29.11.2022, p. 23.	
Recital 71a				
81a		<i>(71a) The Commission should amend the legislative financial statement accompanying this Regulation by providing ENISA with nine additional full-time equivalent and corresponding additional appropriations in order to fulfil its additional tasks provided for in this Regulation.</i>		
Formula				
82	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION: Text Origin: Commission Proposal
CHAPTER I				
83	CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 1				
84	Article 1 Subject matter	Article 1 Subject matter	Article 1 Subject matter	Article 1 Subject matter Text Origin: Commission Proposal
Article 1, first paragraph				
85	This Regulation lays down:	This Regulation lays down:	This Regulation lays down:	This Regulation lays down: Text Origin: Commission Proposal
Article 1, first paragraph, point (a)				
86	(a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;	(a) rules for the ~~placing~~ making available on the market of products with digital elements to ensure the cybersecurity of such products;	(a) rules for the ~~placing~~ making available on the market of products with digital elements to ensure the cybersecurity of such products;	(a) rules for the ~~placing~~ making available on the market of products with digital elements to ensure the cybersecurity of such products; Text Origin: EP Mandate
Article 1, first paragraph, point (b)				
87	(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;	(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;	(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;	(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 1, first paragraph, point (c)				
88	(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;	(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;	(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;	(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes; Text Origin: Commission Proposal
Article 1, first paragraph, point (d)				
89	(d) rules on market surveillance and enforcement of the above-mentioned rules and requirements.	(d) rules on market <u>monitoring</u> , surveillance and enforcement of the above-mentioned rules and requirements.	(d) rules on market surveillance and enforcement of the above-mentioned rules and requirements.	(d) rules on market surveillance, <u>including monitoring</u> , and enforcement of the above-mentioned rules and requirements. Text Origin: EP Mandate
Article 2				
90	Article 2 Scope	Article 2 Scope	Article 2 Scope	Article 2 Scope Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 2(1)				
91	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~~ <u>made available on the market that can have</u> 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 a device or network.	1. This Regulation applies to products with digital elements <u>made available on the market</u> , whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. EP to check 'intended ... use'/'can have' Text Origin: Commission Proposal
Article 2(2)				
92	2. This Regulation does not apply to products with digital elements to which the following Union acts apply:	2. This Regulation does not apply to products with digital elements to which the following Union <u>legislative</u> acts apply:	2. This Regulation does not apply to products with digital elements to which the following Union acts apply:	2. This Regulation does not apply to products with digital elements to which the following Union <u>legal</u> acts apply: Text Origin: Commission Proposal
Article 2(2), point (a)				
93	(a) Regulation (EU) 2017/745;	(a) Regulation (EU) 2017/745;	(a) Regulation (EU) 2017/745;	(a) Regulation (EU) 2017/745; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 2(2), point (b)				
G 94	(b) Regulation (EU) 2017/746;	(b) Regulation (EU) 2017/746;	(b) Regulation (EU) 2017/746;	(b) Regulation (EU) 2017/746; Text Origin: Commission Proposal
Article 2(2), point (c)				
G 95	(c) Regulation (EU) 2019/2144.	(c) Regulation (EU) 2019/2144.	(c) Regulation (EU) 2019/2144.	(c) Regulation (EU) 2019/2144. Text Origin: Commission Proposal
Article 2(3)				
G 96	3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.	3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.	3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.	3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139. Text Origin: Commission Proposal
Article 2(3a)				
Y 96a			3a. This Regulation does not apply to equipment that falls within the scope of Directive 2014/90/EU of the European Parliament and of the Council¹. 1. Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257,	EP check

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			28.8.2014, p. 146).	
	Article 2(3b)			
Y	96b	<u>3a. This Regulation applies to free and open-source software only where such software is made available on the market in the course of a commercial activity.</u>		'Open-source package' to be discussed later, including recitals. COM to propose text.
	Article 2(4), first subparagraph			
G	97	4. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:	4. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:	4. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where: Text Origin: Commission Proposal
	Article 2(4), first subparagraph, point (a)			
G	98	(a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and	(a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and	(a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 2(4), first subparagraph, point (b)			
G	99	(b) the sectoral rules achieve the same level of protection as the one provided for by this Regulation.	(b) the sectoral rules achieve the same or a higher level of protection as the one provided for by this Regulation.	(b) the sectoral rules achieve the same or a higher level of protection as the one provided for by this Regulation. Text Origin: Council Mandate
	Article 2(4), second subparagraph			
Y	100	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.	~~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.~~	Council to provide more (legal) information
	Article 2(4), second subparagraph a			
Y	100a	<u>4a. This Regulation does not apply to spare parts that are exclusively manufactured to replace identical parts and that are supplied by the manufacturer of the original products with digital elements.</u>	4a. This Regulation does not apply to components that are exclusively manufactured as spare parts to replace identical components and are supplied by the manufacturer of the original product with digital elements following the same development and production processes as the original product.	COM to check against NLF.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 2(5)				
Y	101	5. This Regulation does not apply to products with digital elements developed exclusively for national security or military purposes or to products specifically designed to process classified information.	5. This Regulation does not apply to products with digital elements developed or modified exclusively for national security, public security, defence or military purposes or to products specifically designed to process classified information.	Council to provide text.
Article 3				
G	102	Article 3 Definitions	Article 3 Definitions	Article 3 Definitions Text Origin: Commission Proposal
Article 3, first paragraph				
G	103	For the purposes of this Regulation, the following definitions apply:	For the purposes of this Regulation, the following definitions apply:	For the purposes of this Regulation, the following definitions apply: Text Origin: Commission Proposal
Article 3, first paragraph, point (1)				
G	104	(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 ~~and~~ including its remote data processing solutions, ~~including~~ and software or hardware components to be placed on the	(1) ‘product with digital elements’ means any software or hardware product ~~and~~ including its remote data processing solutions, ~~including~~ and software or hardware components to be placed on the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			market separately;	market separately; Text Origin: Council Mandate
Article 3, first paragraph, point (2)				
y	105 (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;	(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~~ <u>or on behalf of</u> the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;	(2) ‘remote data processing’ means any data processing at a distance for which the software or hardware is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;	Council to provide technical arguments for 'hardware'
Article 3, first paragraph, point (3)				
y	106 (3) ‘critical product with digital elements’ means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III;	(3) ‘critical product with digital elements’ means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III;	<i>deleted</i>	To be aligned with Article 6.
Article 3, first paragraph, point (4)				
y	107 (4) ‘highly critical product with digital elements’ means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article	(4) ‘highly critical product with digital elements’ means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article	<i>deleted</i>	To be aligned with Article 6.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	6(5);	6(5);		
Article 3, first paragraph, point (4a)				
107a		<u>(4a) ‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;</u>		<u>(4a) ‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;</u> identical to line 143e Text Origin: EP Mandate
Article 3, first paragraph, point (5)				
108	(5) ‘operational technology’ means programmable digital systems or devices that interact with the physical environment or manage devices that interact with the physical environment;	(5) ‘operational technology’ means programmable digital systems or devices that interact with the physical environment or manage devices that interact with the physical environment;	(5) ‘operational technology’ means programmable digital systems or devices that interact with the physical environment or manage devices that interact with the physical environment;	(5) ‘operational technology’ means programmable digital systems or devices that interact with the physical environment or manage devices that interact with the physical environment; Text Origin: Commission Proposal
Article 3, first paragraph, point (6)				
109	(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;	(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; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 3, first paragraph, point (7)				
110	(7) 'hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data;	(7) 'hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data;	(7) 'hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data;	(7) 'hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data; Text Origin: Commission Proposal
Article 3, first paragraph, point (8)				
111	(8) 'component' means software or hardware intended for integration into an electronic information system;	(8) 'component' means software or hardware intended for integration into an electronic information system;	(8) 'component' means software or hardware intended for integration into an electronic information system;	(8) 'component' means software or hardware intended for integration into an electronic information system; Text Origin: Commission Proposal
Article 3, first paragraph, point (9)				
112	(9) 'electronic information system' means any system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;	(9) 'electronic information system' means any system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;	(9) 'electronic information system' means any system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;	(9) 'electronic information system' means any system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data; Text Origin: Commission Proposal
Article 3, first paragraph, point (10)				
113	(10) 'logical connection' means a	(10) 'logical connection' means a	(10) 'logical connection' means a	(10) 'logical connection' means a

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	virtual representation of a data connection implemented through a software interface;	virtual representation of a data connection implemented through a software interface;	virtual representation of a data connection implemented through a software interface;	virtual representation of a data connection implemented through a software interface; Text Origin: Commission Proposal
Article 3, first paragraph, point (11)				
114	(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, wires or radio waves;	(11) ‘physical connection’ means any connection between electronic information systems or components implemented using physical means, including through electrical, optical or mechanical interfaces, wires or radio waves;	(11) ‘physical connection’ means any connection between electronic information systems or components implemented using physical means, including through electrical, <u>optical</u> or mechanical interfaces, wires or radio waves; Text Origin: Council Mandate
Article 3, first paragraph, point (12)				
115	(12) ‘indirect connection’ means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network;	(12) ‘indirect connection’ means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network;	(12) ‘indirect connection’ means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network;	(12) ‘indirect connection’ means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network; Text Origin: Commission Proposal
Article 3, first paragraph, point (13)				
116	(13) ‘privilege’ means an access right granted to particular users or	(13) ‘privilege’ means an access right granted to particular users or	(13) ‘privilege’ means an access right granted to particular users or	(13) ‘privilege’ means an access right granted to particular users or

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	programmes to perform security-relevant operations within an electronic information system;	programmes to perform security-relevant operations within an electronic information system;	programmes to perform security-relevant operations within an electronic information system;	programmes to perform security-relevant operations within an electronic information system; Text Origin: Commission Proposal
Article 3, first paragraph, point (14)				
117	(14) ‘elevated privilege’ means an access right granted to particular users or programmes to perform an extended set of security-relevant operations within an electronic information system that, if misused or compromised, could allow a malicious actor to gain wider access to the resources of a system or organisation;	(14) ‘elevated privilege’ means an access right granted to particular users or programmes to perform an extended set of security-relevant operations within an electronic information system that, if misused or compromised, could allow a malicious actor to gain wider access to the resources of a system or organisation;	(14) ‘elevated privilege’ means an access right granted to particular users or programmes to perform an extended set of security-relevant operations within an electronic information system that, if misused or compromised, could allow a malicious actor to gain wider access to the resources of a system or organisation;	(14) ‘elevated privilege’ means an access right granted to particular users or programmes to perform an extended set of security-relevant operations within an electronic information system that, if misused or compromised, could allow a malicious actor to gain wider access to the resources of a system or organisation; Text Origin: Commission Proposal
Article 3, first paragraph, point (15)				
118	(15) ‘endpoint’ means any device that is connected to a network and serves as an entry point to that network;	(15) ‘endpoint’ means any device that is connected to a network and serves as an entry point to that network;	(15) ‘endpoint’ means any device that is connected to a network and serves as an entry point to that network;	(15) ‘endpoint’ means any device that is connected to a network and serves as an entry point to that network; Text Origin: Commission Proposal
Article 3, first paragraph, point (16)				
119	(16) ‘networking or computing	(16) ‘networking or computing	(16) ‘networking or computing	(16) ‘networking or computing

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	resources' means data or hardware or software functionality that is accessible either locally or through a network or another connected device;	resources' means data or hardware or software functionality that is accessible either locally or through a network or another connected device;	resources' means data or hardware or software functionality that is accessible either locally or through a network or another connected device;	resources' means data or hardware or software functionality that is accessible either locally or through a network or another connected device; Text Origin: Commission Proposal
Article 3, first paragraph, point (17)				
120	(17) 'economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations laid down by this Regulation;	(17) 'economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations laid down by this Regulation;	(17) 'economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations ~~laid down by~~ in relation to the manufacture of products or making them available on the market in accordance with this Regulation;	(17) 'economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations ~~laid down by~~ <u>in relation to the manufacture of products or making them available on the market in accordance with</u> this Regulation; Text Origin: Council Mandate
Article 3, first paragraph, point (18)				
121	(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, <u>monetisation</u> 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 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, <u>monetisation</u> or free of charge;

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: EP Mandate
Article 3, first paragraph, point (19)				
122	(19) ‘authorised representative’ means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his or her behalf in relation to specified tasks;	(19) ‘authorised representative’ means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his or her behalf in relation to specified tasks;	(19) ‘authorised representative’ means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his or her behalf in relation to specified tasks;	(19) ‘authorised representative’ means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his or her behalf in relation to specified tasks; Text Origin: Commission Proposal
Article 3, first paragraph, point (20)				
123	(20) ‘importer’ means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union;	(20) ‘importer’ means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union;	(20) ‘importer’ means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union;	(20) ‘importer’ means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union; Text Origin: Commission Proposal
Article 3, first paragraph, point (21)				
124	(21) ‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its	(21) ‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its	(21) ‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its	(21) ‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	properties;	properties;	properties;	properties; Text Origin: Commission Proposal
Article 3, first paragraph, point (21a)				
124a		<u>(21b) 'consumer' means any natural person who, under the circumstances of this Regulation, is acting for purposes which are outside their trade, business, craft or profession;</u>	(21a) 'consumer' means any natural person who acts for purposes which are outside that person's trade, business, craft or profession;	<u>(21a) 'consumer' means any natural person who acts for purposes which are outside that person's trade, business, craft or profession;</u> Text Origin: Council Mandate
Article 3, first paragraph, point (21b)				
124b		<u>(21a) 'microenterprises', 'small enterprises' and 'medium sized enterprises' means microenterprises, small enterprises and medium-sized enterprises as defined in Commission Recommendation 2003/361/EC¹;</u> <u>1. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003)1422) (OJ L 124, 20.5.2003, p. 36).</u>		<u>(21b) 'microenterprises', 'small enterprises' and 'medium sized enterprises' means microenterprises, small enterprises and medium-sized enterprises as defined in Commission Recommendation 2003/361/EC¹;</u> <u>1. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003)1422) (OJ L 124, 20.5.2003, p. 36).</u> see similar Council text, line 143d Text Origin: EP Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 3, first paragraph, point (21c)				
Y	124c	<u>(21c) ‘support period’ means the period during which the manufacturer ensures that vulnerabilities of the product with digital elements are handled effectively and in accordance with the essential requirements set out in Annex I, Section 2;</u>	PUBLIC	To be aligned to Article 10
Article 3, first paragraph, point (22)				
G	125	(22) ‘placing on the market’ means the first making available of a product with digital elements on the Union market;	(22) ‘placing on the market’ means the first making available of a product with digital elements on the Union market;	(22) ‘placing on the market’ means the first making available of a product with digital elements on the Union market; Text Origin: Commission Proposal
Article 3, first paragraph, point (23)				
G	126	(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, 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, whether in return for payment or free of charge; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 3, first paragraph, point (24)				
127	(24) ‘intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;	(24) ‘intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;	(24) ‘intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;	(24) ‘intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation; Text Origin: Commission Proposal
Article 3, first paragraph, point (25)				
128	(25) ‘reasonably foreseeable use’ means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions;	(25) ‘reasonably foreseeable use’ means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions;	(25) ‘reasonably foreseeable use’ means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions;	(25) ‘reasonably foreseeable use’ means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions; Text Origin: Commission Proposal
Article 3, first paragraph, point (26)				
129	(26) ‘reasonably foreseeable	(26) ‘reasonably foreseeable	(26) ‘reasonably foreseeable	(26) ‘reasonably foreseeable

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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;	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;	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;	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; Text Origin: Commission Proposal
Article 3, first paragraph, point (27)				
130	(27) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;	(27) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;	(27) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;	(27) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring; Text Origin: Commission Proposal
Article 3, first paragraph, point (28)				
131	(28) ‘conformity assessment’ means the process of verifying whether the essential requirements set out in Annex I have been fulfilled;	(28) ‘conformity assessment’ means the process of verifying whether the essential requirements set out in Annex I have been fulfilled;	(28) ‘conformity assessment’ means the process of verifying whether the essential requirements set out in Annex I have been fulfilled;	(28) ‘conformity assessment’ means the process of verifying whether the essential requirements set out in Annex I have been fulfilled; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 3, first paragraph, point (29)				
132	(29) ‘conformity assessment body’ means a body defined in Article 2(13) of Regulation (EU) No 765/2008;	(29) ‘conformity assessment body’ means a body defined in Article 2(13) of Regulation (EU) No 765/2008;	(29) ‘conformity assessment body’ means a conformity assessment body as body defined in Article 2, point (13) , (13) of Regulation (EU) No 765/2008;	(29) ‘conformity assessment body’ means a <u>conformity assessment body as body</u> defined in Article 2, <u>point (13), (13)</u> of Regulation (EU) No 765/2008; Text Origin: Council Mandate
Article 3, first paragraph, point (30)				
133	(30) ‘notified body’ means a conformity assessment body designated in accordance with Article 33 of this Regulation and other relevant Union harmonisation legislation;	(30) ‘notified body’ means a conformity assessment body designated in accordance with Article 33 of this Regulation and other relevant Union harmonisation legislation;	(30) ‘notified body’ means a conformity assessment body designated in accordance with Article 33 of this Regulation and other relevant Union harmonisation legislation;	(30) ‘notified body’ means a conformity assessment body designated in accordance with Article 33 of this Regulation and other relevant Union harmonisation legislation; Text Origin: Commission Proposal
Article 3, first paragraph, point (31)				
134	(31) ‘substantial modification’ means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed;	(31) ‘substantial modification’ means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed, <u>excluding necessary security updates that aim to</u>	(31) ‘substantial modification’ means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended ~~use~~ purpose for which the product with digital elements has been assessed;	(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~~ <u>purpose</u> for which the product with digital elements has been assessed, <u>excluding necessary security</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>mitigate vulnerabilities</u> ;		<u>updates that aim to mitigate vulnerabilities</u> ; Text in () to be continued together with separation security/functional up-dates and related recitals Text Origin: EP Mandate
Article 3, first paragraph, point (32)				
135	(32) ‘CE marking’ means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential requirements set out in Annex I and other applicable Union legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;	(32) ‘CE marking’ means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential requirements set out in Annex I and other applicable Union legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;	(32) ‘CE marking’ means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential requirements set out in Annex I and other applicable Union legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;	(32) ‘CE marking’ means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential requirements set out in Annex I and other applicable Union ~~legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’)~~ providing for its affixing; Text Origin: Council Mandate
Article 3, first paragraph, point (32a)				
135a			(32a) ‘Union harmonisation legislation’ means Union legislation listed in Annex I to Regulation (EU) 2019/1020 and any other Union legislation harmonising the conditions for the marketing of products to which that Regulation applies;	<u>(32a) ‘Union harmonisation legislation’ means Union legislation listed in Annex I to Regulation (EU) 2019/1020 and any other Union legislation harmonising the conditions for the marketing of products to which that Regulation applies;</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Council Mandate
	Article 3, first paragraph, point (33)			
G	136	(33) ‘market surveillance authority’ means the authority as defined in Article 3, point (4) of Regulation (EU) 2019/1020;	(33) ‘market surveillance authority’ means the authority as defined in Article 3, point (4) of Regulation (EU) 2019/1020;	(33) ‘market surveillance authority’ means <u>a market surveillance</u> ~~the~~ authority as defined in Article 3, point (4), of Regulation (EU) 2019/1020; Text Origin: Council Mandate
	Article 3, first paragraph, point (34)			
G	137	(34) ‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012;	(34) ‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012;	(34) ‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012; Text Origin: Commission Proposal
	Article 3, first paragraph, point (34a)			
Y	137a		<u>(34a) ‘international standard’ means an international standard as defined in Article 2, point (1)(a) of Regulation (EU) No 1025/2012;</u>	To be aligned with agreed text
	Article 3, first paragraph, point (35)			
Y	138	(35) ‘cybersecurity risk’ means risk as defined in Article [Article X] of	(35) ‘ ~~cybersecurity~~ risk’ means risk as defined in Article ~~[Article X]~~ <u>6</u> .	(35) ‘cybersecurity risk’ means risk as defined in Article [Article] EP check (LS)

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Directive [Directive XXX/XXXX (NIS2)];	<u>point (9)</u> of Directive ~~Directive XXX/XXXX (NIS2EU)~~ <u>2022/2555</u> ;	~~X~~ 6, <u>point (9)</u> , of Directive ~~Directive XXX/XXXX (NIS2EU)~~ <u>2022/2555</u> ;	
Article 3, first paragraph, point (36)				
139	(36) ‘significant cybersecurity risk’ means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;	(36) ‘significant cybersecurity risk’ means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;	(36) ‘significant cybersecurity risk’ means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;	(36) ‘significant cybersecurity risk’ means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption; Text Origin: Commission Proposal
Article 3, first paragraph, point (37)				
140	(37) ‘software bill of materials’ means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;	(37) ‘software bill of materials’ <u>or</u> <u>‘SBOM’</u> means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;	(37) ‘software bill of materials’ means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;	(37) ‘software bill of materials’ <u>or</u> <u>‘SBOM’</u> means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements; Text Origin: EP Mandate
Article 3, first paragraph, point (38)				
141	(38) ‘vulnerability’ means a vulnerability as defined in Article [Article X] of Directive [Directive	(38) ‘vulnerability’ means a vulnerability as defined in Article ~~Article X~~ <u>6, point (15)</u> of Directive	(38) ‘vulnerability’ means a vulnerability as defined in Article [Article X] of Directive ~~6, point~~	(38) ‘vulnerability’ means a vulnerability as defined in Article ~~Article X~~ <u>of Directive 6, point</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	XXX/XXXX (NIS2)];	~~/Directive XXX/XXXX (NIS2 EU)/~~ <u>2022/2555;</u>	(15), of Directive ~~XXX/XXXX~~ (NIS2 (EU)) 2022/2555;	<u>(15), of</u> Directive ~~XXX/XXXX (NIS2~~ <u>(EU) 2022/2555;</u> Text Origin: Council Mandate
Article 3, first paragraph, point (38a)				
y	141a		(38a) ‘exploitable vulnerability’ means a vulnerability as defined in Article 6, point (15), of Directive (EU) 2022/2555 that has the potential to be effectively used by an adversary under practical operational conditions;	To be aligned/discussed with Annex I
Article 3, first paragraph, point (39)				
y	142	(39) ‘actively exploited vulnerability’ means a vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner;	(39) ‘actively exploited vulnerability’ means a vulnerability as defined in Article 6, point (15), of Directive (EU) 2022/2555 for which there is reliable evidence that ~~execution of a malicious code was performed by an actor on~~ an actor has attempted to exploit it in a system without permission of the system owner, irrespective of whether this attempt has been successful or not;	To be further discussed - EP and Council check
Article 3, first paragraph, point (39a)				
y	142a			To be aligned with Article 11 and 11a

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement	
	Article 3, first paragraph, point (39b)				
Y	142b	<u>(39b) ‘near miss’ means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;</u>		To be aligned with Article 11 and 11a	Y
	Article 3, first paragraph, point (39c)				
Y	142c	<u>(39c) ‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;</u>		To be aligned with Article 11 and 11a	Y
	Article 3, first paragraph, point (40)				
G	143	(40) ‘personal data’ means data as defined in Article 4(1) of Regulation (EU) 2016/679.	(40) ‘personal data’ means data as defined in Article ~~4(1)~~ <u>4, point (1)</u> , of Regulation (EU) 2016/679.	(40) ‘personal data’ means personal data as defined in Article ~~4(1)~~ <u>4, point (1)</u> , of Regulation (EU) 2016/679. Text Origin: Council Mandate	G
	Article 3, first paragraph, point (40a)				
G	143a		(41) ‘recall’ means recall as defined in Article 3, point (22), of Regulation (EU) 2019/1020;	<u>(41) ‘recall’ means recall as defined in Article 3, point (22), of Regulation (EU) 2019/1020;</u> Text Origin: Council Mandate	G
	Article 3, first paragraph, point (40b)				
G	143b		(42) ‘withdrawal’ means	<u>(42) ‘withdrawal’ means</u>	G

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			withdrawal as defined in Article 3, point (23), of Regulation (EU) 2019/1020.	<u>withdrawal as defined in Article 3, point (23), of Regulation (EU) 2019/1020.</u> Text Origin: Council Mandate
	Article 3, first paragraph, point (40c)			
Y	143c		(43) 'incident having an impact on the security of the product with digital elements' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555 which negatively affects the ability of a manufacturer's product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions.	To be further discussed / alignment to Article 11
	Article 3, first paragraph, point (40d)			
G	143d		(44) 'micro, small and medium-sized enterprises' or 'SMEs' means micro, small and medium-sized enterprises as defined in the Annex to Recommendation 2003/361/EC;	see line 124b
	Article 3, first paragraph, point (40e)			
G	143e		(45) 'cybersecurity' means cybersecurity as defined in Article	see line 107a

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			2, point (1), of Regulation (EU) 2019/881.	
	Article 4			
G	144	Article 4 Free movement	Article 4 Free movement	Article 4 Free movement Text Origin: Commission Proposal
	Article 4(1)			
G	145	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 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 which comply with this Regulation. Text Origin: Commission Proposal
	Article 4(1a)			
Y	145a		1a. In accordance with paragraph 1, this Regulation shall not prevent Member States from subjecting products with digital elements to additional cybersecurity requirements for the procurement or use of those products for specific purposes, provided that such requirements are consistent with Member States' obligations	To be discussed together with lines 176a-c.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			laid down in Union law.	
Article 4(2)				
146	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 <u>prototype</u> product with digital elements which does not comply with this Regulation, <u>provided that the availability of such a product is limited in time and geographical area and is supplied exclusively for testing and, where possible, a visible sign indicating its non-compliance.</u>	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.	EP check
Article 4(3)				
147	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 <u>free of charge</u> 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 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.	EP check

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 4(3a)			
Y	147a		4. Paragraph 3 does not apply to safety components as specified under other Union harmonisation legislation.	Council check
	Article 4(3b)			
Y	147b		5. This Regulation shall not prevent Member States from subjecting products with digital elements to additional measures when these products will be used for military, defence or national security purposes, and such measures are necessary and proportionate for the achievement of those purposes.	Council to reflect and propose text for lines 147b and 145a - to be discussed together with lines 176a-c
	Article 4(3c)			
Y	147c		6. The obligations laid down in this Regulation shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.	Council check

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 4(3d)				
147d		<u>3a. Member States, if applicable with the support of ENISA, may establish controlled testing environments for innovative products to facilitate their development. In that context, particular support shall be provided for microenterprises, small and medium-sized enterprises, including start-ups.</u>		<u>3a. Member States, if applicable with the support of ENISA, may establish controlled testing environments for innovative products to facilitate their development and to comply with this Regulation. Where relevant, support shall be provided for microenterprises, small and medium-sized enterprises, including start-ups.</u> COM may provide up-dated text. Placement of text to be defined together with Article 24a. Text Origin: EP Mandate
Article 5				
148	Article 5 Requirements for products with digital elements	Article 5 Requirements for products with digital elements	Article 5 Requirements for products with digital elements	Article 5 Requirements for products with digital elements Text Origin: Commission Proposal
Article 5, first paragraph				
149	Products with digital elements shall only be made available on the market where:	Products with digital elements shall only be made available on the market where:	Products with digital elements shall only be made available on the market where:	Products with digital elements shall only be made available on the market where: Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Article 5, first paragraph, point (1)				
150	(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated, and	(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, <u>updated</u> <u>provided with the necessary security and functionality updates</u> , and	(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated, and	(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, <u>updated</u> <u>having installed the necessary security updates</u> , and Text Origin: EP Mandate
Article 5, first paragraph, point (2)				
151	(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I.	(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I.	(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I.	(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I. Text Origin: Commission Proposal
Article 6				
152	Article 6 Critical products with digital elements	Article 6 Critical products with digital elements	Article 6 ~~Critical~~ Classification of products with digital elements subject to specific conformity assessment procedures	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 6(1)				
153	1. Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products.	1. Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products. <u><i>The integration of a product of higher class of criticality does not change the level of criticality for the product into which it is integrated.</i></u>	1. Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products subject to the conformity assessment procedures referred to in Article 24 (2) and (3).	
Article 6(1a)				
153a			1a. The categories of products with digital elements referred to in paragraph 1 are divided into class I and class II as set out in Annex III The categories of products with digital elements listed in class I of Annex III meet one of the following criteria:	

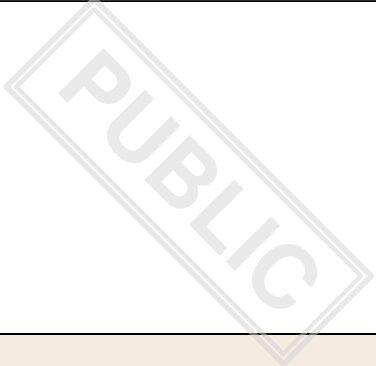
	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 6(1a), first subparagraph, point (a)				
153b			(a) the product with digital elements performs primarily functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;	
Article 6(1a), first subparagraph, point (b)				
153c			(b) the product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health and safety of a large number of individuals through direct manipulation, such as a central system function, including network management, configuration control, virtualisation, processing of personal data.	
Article 6(1a), second subparagraph				
153d			The categories of products with digital elements listed in class II of Annex III meet both criteria	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			referred to in points (a) and (b) of this paragraph.	
Article 6(2)				
154	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. <u>The first such delegated act may be adopted no earlier than two years after the date of entry into force of this Regulation. Any subsequent delegated act may be adopted at the earliest two years thereafter.</u> 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~~ within each class of the categories of products with digital elements a new category and specifying its definition, moving a category of products from one class to the other 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 cybersecurity-related functionalities or the function and the level of cybersecurity risk posed by the products with digital elements as set out by the criteria ~~shall be taken into account; referred to in paragraph 1a.~~	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 6(2), point (a)				
155	(a) the cybersecurity-related functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:	(a) the cybersecurity-related functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:	<i>deleted</i>	
Article 6(2), point (a)(i)				
156	(i) it is designed to run with elevated privilege or manage privileges;	(i) it is designed to run with elevated privilege or manage privileges;	<i>deleted</i>	
Article 6(2), point (a)(ii)				
157	(ii) it has direct or privileged access to networking or computing resources;	(ii) it has direct or privileged access to networking or computing resources;	<i>deleted</i>	
Article 6(2), point (a)(iii)				
158	(iii) it is designed to control access to data or operational technology;	(iii) it is designed to control access to data or operational technology;	<i>deleted</i>	
Article 6(2), point (a)(iv)				
159	(iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection.	(iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection.	<i>deleted</i>	
Article 6(2), point (b)				

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
160	(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 sensitive environments, including in industrial settings or by essential entities of the type referred to in the ~~Annex [Annex I] to the Directive [Article 3 of Directive XXX/XXXX (NIS2 (EU))]~~ 2022/2555 ;	<i>deleted</i>	
Article 6(2), point (c)				
161	(c) the intended use of performing critical or sensitive functions, such as processing of personal data;	(c) the intended use of performing critical or sensitive functions, such as processing of personal data;	<i>deleted</i>	
Article 6(2), point (d)				
162	(d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;	(d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;	<i>deleted</i>	
Article 6(2), point (e)				
163	(e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact.	(e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact.	<i>deleted</i>	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 6(3)				
164	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 12 months since~~ <u>by ... [6 months after</u> 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~~ By ... [18 months after the date of entry into force of this Regulation], the Commission shall adopt an implementing act specifying the definitions of the ~~product categories~~ categories of products with digital elements under class I and class II as set out in Annex III. ~~The delegated and the definitions of the categories of products with digital elements set out in Annex IIIa.~~ That implementing act shall be adopted [by 12 months since the entry into force of this Regulation] in accordance with the examination procedure referred to in Article 51(2).	
Article 6(4)				
165	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). <u>Where a new category of critical products with digital elements is added to class I or II as set out in Annex III by means of a delegated</u>	<i>deleted</i>	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>act pursuant to paragraph 2 of this Article, it shall be subject to the relevant conformity assessment procedures referred to in Article 24(2) and (3) of this Regulation within 12 months of the date of adoption of the delegated act concerned.</u>		
Article 6a				
165a			Article 6a Required use of European cybersecurity certification schemes	
Article 6a(1)				
165b			1. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation to determine which products with digital elements that have the core functionality of a category that is listed in Annex IIIa to this Regulation shall be required to obtain a European cybersecurity certificate at a specified assurance under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I to	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			this Regulation or parts thereof, provided that a European cybersecurity certification scheme covering those categories of products with digital elements has been adopted pursuant to Regulation (EU) 2019/881, and is available to manufacturers. The delegated acts shall specify the required assurance level that shall be proportionate to the level of cybersecurity risk associated with the products with digital elements and shall take account of their intended purpose, including their critical dependency by entities of a type referred to in Annex I to Directive (EU) 2022/2555.	
Article 6a(1), first subparagraph				
165c			Before adopting such delegated acts and provided that a European cybersecurity certification scheme as referred to in the first subparagraph of this paragraph is available, the Commission shall carry out an impact assessment analysing the potential market impact of the envisaged measures and shall carry out consultations with relevant stakeholders, including the European Cybersecurity Certification Group referred to in Regulation (EU) 2019/881. The impact assessment	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			shall also take into account the intended purpose of the products with digital elements considered to be subject to such measures, including the extent to which there is a critical dependency on these products of entities of a type referred to in Annex I to Directive (EU) 2022/2555, and include an analysis of both the supply and demand side as well as the readiness and the capacity level of the Member States for the implementation of the respective European cybersecurity certification scheme. Where no delegated act as referred to in the first subparagraph has been adopted, products with digital elements which have the core functionality of a category listed in Annex IIIa shall be subject to the conformity assessment procedures referred to in Article 24 (3).	
Article 6a(1), second subparagraph				
165d			The delegated acts referred to in the first subparagraph shall provide for an adequate transition period for their application.	
Article 6(5)				
166	5. The Commission is empowered	5. The Commission is empowered	~~52.~~ The Commission is empowered	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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:	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 <u>at assurance level 'high'</u> pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. <u>The obligation to obtain a European cybersecurity certificate shall apply within 12 months of the adoption of the relevant delegated act.</u> 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:	to adopt delegated acts in accordance with Article 50 to ~~supplement this Regulation by specifying~~ amend Annex IIIa by adding or withdrawing 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 and the required assurance level, the Commission shall take into account the ~~level of cybersecurity risk related to~~ criteria referred to in Article 6 (1a) as well as and ensure that the category of products with digital elements, ~~in light of one or several~~ meet at least one of the ~~criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is~~ following criteria:	
Article 6(5), point (a)				
167	(a) used or relied upon by the essential entities of the type referred to in Annex [Annex I] to the	(a) used or relied upon by the essential entities of the type referred to in ~~Annex [Annex I] to the~~ <u>Article 3</u>	(a) ~~used or relied upon by the essential~~ the extent to which there is a critical dependency of entities	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Directive [Directive XXX/ XXXX (NIS2)] or will have potential future significance for the activities of these entities; or	<del>of Directive ~~Directive XXX/ XXXX~~ (NIS2EU) 2022/2555</del> or will have potential future significance for the activities of these entities; or	of the type referred to in Annex [Annex I] to the Directive [to Directive XXX/ XXXX (NIS2EU)] or will have potential future significance for the activities of these entities; or 2022/2555 on the category of products with digital elements ;	
Article 6(5), point (b)				
168	(b) relevant for the resilience of the overall supply chain of products with digital elements against disruptive events.	(b) relevant for the resilience of the overall supply chain of products with digital elements against disruptive events. <u><i>5a. The Commission is empowered to adopt the delegated acts referred to in paragraph 5 of this Article no earlier than 12 months after the adoption of the relevant European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881.</i></u>	(b) ~~relevant for the resilience of the overall supply chain~~ the extent to which cybersecurity incidents and exploited vulnerabilities concerning the category of products with digital elements against disruptive events can lead to serious disruptions to critical supply chains across the internal market.	
Article 6a(2), second subparagraph				
168a			Before adopting such delegated acts, the Commission shall carry out an impact assessment of the type referred to in paragraph 1.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 6a(2), third subparagraph			
	168b		The delegated acts referred to in the first subparagraph shall provide for an adequate transition period for their application.	
	Article 6a			
Y	168c	<u>Article 6a</u> <u>Expert Group on cyber resilience</u>		EP to provide revised text
	Article 6a, first paragraph			
Y	168d	<u>1. By ... /6 months after the date of entry into force of this Regulation], the Commission shall establish an expert group on cyber resilience (the 'Expert Group'). The Expert Group shall be appointed for a renewable three-year term by the Commission. The composition of the Expert Group shall aim to be gender and geographically balanced and shall include the following:</u>		
	Article 6a, second paragraph			
Y	168e	<u>(a) representatives of each of the following:</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 6a, third paragraph			
Y	168f	<u>(i) the European Union Agency for Cybersecurity;</u>		Y
	Article 6a, fourth paragraph			
Y	168g	<u>(ii) the European Cybersecurity Competence Centre;</u>		Y
	Article 6a, fifth paragraph			
Y	168h	<u>(iii) the European Data Protection Board;</u>		Y
	Article 6a, sixth paragraph			
Y	168i	<u>(iv) European standardisation bodies.</u>		Y
	Article 6a, seventh paragraph			
Y	168j	<u>Where needed, representatives of other Union Agencies may be invited.</u>		Y
	Article 6a, first paragraph, point (b)			
Y	168k	<u>(b) experts representing relevant economic operators, ensuring the adequate representation of microenterprises and small and</u>		Y

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>medium-sized enterprises;</u>		
	Article 6a, seventh paragraph, point (b)			
Y	168l	<u>(c) experts representing civil society, including consumer organisations and the free and open-source community;</u>		Y
	Article 6a, seventh paragraph, point (c)			
Y	168m	<u>(d) experts appointed in a personal capacity, who have proven knowledge and experience in the areas covered by this Regulation;</u>		Y
	Article 6a, seventh paragraph, point (d)			
Y	168n	<u>(e) experts representing academia, including universities, research institutes and other scientific organisations, including persons with global expertise.</u>		Y
	Article 6a, eighth paragraph			
Y	168o	<u>2. The Expert Group shall advise the Commission with regard to the following:</u>		Y

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 6a, eighth paragraph, point (a)			
y	168p	<u>(a) the list of critical products with digital elements set out in Annex III, as well as on the possible need to update that list;</u>		y
	Article 6a, eighth paragraph, point (b)			
y	168q	<u>(b) the implementation of European cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 and on the possibility to make them mandatory for highly critical products with digital elements;</u>		y
	Article 6a, eighth paragraph, point (c)			
y	168r	<u>(c) non-binding evaluations of products with digital elements upon request by a market surveillance authority that is conducting an investigation under Article 43;</u>		y
	Article 6a, eighth paragraph, point (d)			
y	168s	<u>(d) the application of relevant concepts of the new legislative framework to software, in particular free and open-source software;</u>		y

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 6a, eighth paragraph, point (e)			
y	168t	<u>(e) the elements of the Regulation to be addressed by the guidelines referred to in Article 17a;</u>		y
	Article 6a, eighth paragraph, point (f)			
y	168u	<u>(f) the availability and the quality of European and international standards, and the possibility to supplement or replace them with common technical specifications;</u>		y
	Article 6a, eighth paragraph, point (g)			
y	168v	<u>(g) the availability of skilled professionals in the field of cybersecurity across the Union, including of adequate personnel to perform third-party conformity assessments pursuant to this Regulation;</u>		y
	Article 6a, eighth paragraph, point (h)			
y	168w	<u>(h) the possible need to amend this Regulation.</u> <u>The Expert Group shall also map trends at Union and Member State level regarding existing and patched vulnerabilities.</u>		y

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 6a, ninth paragraph			
Y	168x	<u>3. The Expert Group shall take into account the views of a wide range of stakeholders and perform their tasks with highest level of professionalism, independence, impartiality and objectivity.</u>		Y
	Article 6a, tenth paragraph			
Y	168y	<u>4. The Commission shall consult the Expert Group when preparing delegated or implementing acts based upon this Regulation.</u>		Y
	Article 6a, eleventh paragraph			
Y	168z	<u>5. The Expert Group may provide market surveillance authorities with non-binding evaluations of products with digital elements to facilitate investigations under Article 43.</u>		Y
	Article 6a, twelfth paragraph			
Y	168aa	<u>6. The Expert Group shall be chaired by the Commission and shall be constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. In that context, the Commission may invite</u>		Y

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>experts with specific expertise on an ad hoc basis.</u>		
Article 6a, thirteenth paragraph				
168ab		<u>7. The Expert Group shall carry out its tasks in accordance with the principle of transparency. The Commission shall publish the composition of the Expert Group, the declaration of interests of its members, a summary of the meetings of the Expert Group and other relevant documents on the Commission website.</u>		
Article 6b				
168ac		<u>Article 6b</u> <u>Enhancing skills in a cyber resilient digital environment</u>		
Article 6b, first paragraph				
168ad		<u>For the purpose of this Regulation and in order to respond to the demand of professionals capable of ensuring the cybersecurity of products with digital elements, the Commission and Member States, in cooperation with ENISA, shall ensure the implementation of:</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement	
Article 6b, first paragraph, point (a)					
168ae		<u>(a) education and training programmes in the cyber security field and their associated career pathways, contributing to making the cyber security workforce more resilient and inclusive, also in terms of gender and aligned with the needs of undertakings concerned, in particular where such undertakings are microenterprises, small or medium-sized enterprises, including start-ups, or public administration;</u>	PUBLIC		
Article 6b, first paragraph, point (b)					
168af		<u>(b) initiatives to increase the collaboration between the private sector, economic operators, including via re-skilling or up-skilling for manufacturers' employees, consumers, education and training providers as well as Member States, expanding the options for young people to access jobs in this sector;</u>			
Article 6b, first paragraph, point (c)					
168ag		<u>(c) strategies aiming to enhance workforce mobility, developing cyber security skills and creating organisational and technological</u>			

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>tools to maximise existent cyber security talent.</u>		
Article 7				
169	Article 7 General product safety	Article 7 General product safety	Article 7 General product safety	Article 7 General product safety Text Origin: Commission Proposal
Article 7, first paragraph				
170	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.	By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation ~~[General Product Safety Regulation]~~ <u>(EU) 2023/988</u> 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~~ <u>Regulation (EU) 2023/988</u> , Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation ~~[General Product Safety Regulation]~~ <u>(EU) 2023/988</u> shall apply to those products with respect to safety risks not covered by this Regulation.	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) EU]~~ of the General Product Safety Regulation <u>2023/988</u> , Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation ~~[General Product Safety Regulation]~~ that shall apply to those products with digital elements with respect to safety risks not covered by this Regulation where those products are not subject to specific requirements laid down in other Union harmonisation legislation as defined in Article 3, point (27) of	By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation ~~[General Product Safety Regulation]~~ <i>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) EU] of the General Product Safety Regulation</i> <u>2023/988</u> , Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of ~~Regulation [General Product Safety Regulation]~~ <i>that</i> shall apply to ~~those~~ products with <u>digital elements with</u> respect to safety risks not covered by this Regulation <u>where those products are not subject to specific requirements laid down in other Union harmonisation legislation as defined in Article 3, point (27) of</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			Regulation (EU) 2023/988.	<u>Regulation (EU) 2023/988.</u> Final IMCO check Text Origin: Council Mandate
Article 8				
171	Article 8 High-risk AI systems	Article 8 High-risk AI systems	Article 8 High-risk AI systems	Article 8 High-risk AI systems Text Origin: Commission Proposal
Article 8(1)				
172	1. Products with digital elements classified as high-risk AI systems in accordance with Article [Article 6] of Regulation [the AI Regulation] which fall within the scope of this Regulation, and fulfil the essential requirements set out in Section 1 of Annex I of this Regulation, and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I, shall be deemed in compliance with the requirements related to cybersecurity set out in Article [Article 15] of Regulation [the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far	1. Products with digital elements classified as high-risk AI systems in accordance with Article [Article 6] of Regulation [the AI Regulation] which fall within the scope of this Regulation, and fulfil the essential requirements set out in Section 1 of Annex I of this Regulation, and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I, shall be deemed in compliance with the requirements related to cybersecurity set out in Article [Article 15] of Regulation [the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far	1. ~~Products with digital elements classified as high-risk AI systems in accordance with~~ Without prejudice to the requirements relating to accuracy and robustness set out in Article [Article 6] ~~15] of Regulation [the AI Regulation], products with digital elements~~ which fall within the scope of this Regulation, ~~and fulfil the essential requirements set out in Section 1 of Annex I of this~~ and which are classified as high-risk AI systems pursuant to Article [Article 6] of Regulation, ~~and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I, [the AI Regulation]~~ shall be deemed ~~in compliance~~ compliant with the	1. ~~Products with digital elements classified as high-risk AI systems in accordance with~~ Without prejudice to the requirements relating to accuracy and robustness set out in Article [Article 6] ~~15] of Regulation [the AI Regulation], products with digital elements~~ which fall within the scope of this Regulation, ~~and fulfil the essential requirements set out in Section 1 of Annex I of this~~ and which are classified as high-risk AI systems pursuant to Article [Article 6] of Regulation, ~~and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I, [the AI Regulation]~~ shall be deemed ~~in compliance~~ compliant with the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.	as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation.	cybersecurity 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. if:	cybersecurity 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. if: Text Origin: Council Mandate
Article 8(1), point (a)				
G	172a		(a) they fulfil the essential requirements set out in Section 1 of Annex I to this Regulation;	<u>(a) they fulfil the essential requirements set out in Section 1 of Annex I to this Regulation;</u> Text Origin: Council Mandate
Article 8(1), point (b)				
G	172b		(b) the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I to this Regulation; and	<u>(b) the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I to this Regulation; and</u> Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 8(1), point (c)				
172c			(c) the achievement of the level of cybersecurity protection required under Article [Article 15] of Regulation [the AI Regulation] is demonstrated in the EU declaration of conformity issued under this Regulation.	<u>(c) the achievement of the level of cybersecurity protection required under Article [Article 15] of Regulation [the AI Regulation] is demonstrated in the EU declaration of conformity issued under this Regulation.</u> Text Origin: Council Mandate
Article 8(2)				
173	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	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~~ <u>relevant</u> 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 <u>that fall</u> 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	2. For the products with digital elements and cybersecurity requirements referred to in paragraph 1, the relevant conformity assessment procedure as required by Article [Article 43] of Regulation [AI Regulation] shall apply. For the purpose of that assessment, notified bodies which are ~~entitled~~ <u>competent</u> to control the conformity of the high-risk AI systems under ~~the~~ Regulation [AI Regulation] shall be also ~~entitled~~ <u>competent</u> to control the conformity of ~~the~~ high-risk AI systems which fall within the scope of this Regulation with the requirements set out in Annex I to this Regulation, provided that the compliance of those notified bodies with the requirements laid down in Article 29 of this Regulation ~~have~~ has been assessed in the context	2. For the products <u>with digital elements</u> 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~~ <u>competent</u> to control the conformity of the high-risk AI systems under ~~the~~ Regulation [AI Regulation] shall be also ~~entitled~~ <u>competent</u> to control the conformity of ~~the~~ high-risk AI systems <u>which fall</u> 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~~ <u>has</u> been assessed in the context

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Regulation [AI Regulation].	Regulation [AI Regulation].	of the notification procedure under Regulation [AI Regulation].	of the notification procedure under Regulation [AI Regulation]. DLA check against final version of AI reg. Text Origin: Council Mandate
Article 8(3)				
174	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 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.	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 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.	3. By way of derogation from paragraph 2, ~~critical~~ products with digital elements listed in Annex III ~~of~~ this Regulation, which ~~have to apply~~ are subject to the conformity assessment procedures referred to in Articles 24(2)(a), 24(2)(b), 24(3)(a) and 24(3)(b) ~~under~~ of this Regulation and which are also classified as high-risk AI systems ~~according~~ pursuant to Article [Article 6] of the Regulation [AI Regulation], and to which the conformity assessment procedure based on internal control referred to in Annex [Annex VI] to Regulation [the AI Regulation] applies, shall be subject to the conformity assessment procedures as required ~~by~~ under this Regulation in so far as the essential requirements of this Regulation are concerned.	3. By <u>way of</u> derogation from paragraph 2, <u>(critical)</u> products with digital elements listed in Annex III <u>of</u> this Regulation, which ~~have to apply~~ <u>are subject to</u> the conformity assessment procedures referred to in Articles 24(2)(a), 24(2)(b), 24(3)(a) and 24(3)(b) ~~under~~ <u>of</u> this Regulation and which are also classified as high-risk AI systems ~~according~~ <u>pursuant</u> 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~~ <u>under</u> this Regulation in so far as the essential requirements of this Regulation are concerned. "(critical)" to be aligned with Article 6 Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 8(3a)				
174a		<u>3a. Manufacturers of products with digital elements classified as high-risk AI systems in accordance with paragraph 1 of this Article may participate in the AI regulatory sandboxes referred to in Article 53 of Regulation [the AI Regulation].</u>		<u>3a. Manufacturers of products with digital elements referred to in paragraph 1 of this Article may participate in the AI regulatory sandboxes referred to in Article 53 of Regulation [the AI Regulation].</u> Text Origin: EP Mandate
Article 9				
175	Article 9 Machinery products	Article 9 Machinery products	deleted	EP check
Article 9, first paragraph				
176	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	Machinery products ~~under that fall within~~ the scope of Regulation ~~[Machinery Regulation proposal]~~ (EU) 2023/1230 which are products with digital elements <u>or partly completed products with digital elements</u> 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]~~ (EU) 2023/1230, as regards protection	deleted	EP check

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement	
	achievement of the level of protection required by those requirements is demonstrated in the EU declaration of conformity issued under this Regulation.	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.	PUBLIC		
Article 9a					
176a		<u>Article 9a</u> <u>Public procurement of products with digital elements</u>			
Article 9a, first paragraph					
176b		<u>1. Without prejudice to Directives 2014/24/EU¹ and 2014/25/EU² of the European Parliament and of the Council, Member States shall ensure, when procuring products with digital elements, a high level of cybersecurity and an appropriate support period.</u> <u>1. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).</u> <u>2. Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).</u>			

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 9a, second paragraph				
176c		<u>2. Member States shall ensure that manufacturers remedy vulnerabilities in publicly procured products with digital elements, including by making security updates available promptly.</u>		
CHAPTER II				
177	CHAPTER II OBLIGATIONS OF ECONOMIC OPERATORS	CHAPTER II OBLIGATIONS OF ECONOMIC OPERATORS	CHAPTER II OBLIGATIONS OF ECONOMIC OPERATORS	CHAPTER II OBLIGATIONS OF ECONOMIC OPERATORS Text Origin: Commission Proposal
Article 10				
178	Article 10 Obligations of manufacturers	Article 10 Obligations of manufacturers	Article 10 Obligations of manufacturers	Article 10 Obligations of manufacturers Text Origin: Commission Proposal
Article 10(1)				
179	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	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	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	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

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	essential requirements set out in Section 1 of Annex I.	essential requirements set out in Section 1 of Annex I.	essential requirements set out in Section 1 of Annex I.	essential requirements set out in Section 1 of Annex I. Text Origin: Commission Proposal
Article 10(2)				
180	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 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 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 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. Text Origin: Commission Proposal
Article 10(2a)				
180a		<u>2a. On the basis of the cybersecurity risk assessment, manufacturers shall determine how the essential requirements set out in Section 1 of Annex I are applicable</u>	2a. The risk assessment referred to in paragraph 2 shall be documented and updated as appropriate during the expected lifetime of the product. It shall	<u>2a. The cybersecurity risk assessment shall be documented and updated as appropriate during the (support period/expected lifetime of the product.) It shall</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>to their product with digital elements. They shall include the risk assessment in the technical documentation as set out in Article 23.</u>	comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use of the product with digital elements, such as the operational environment, and the assets to be protected, taking into account the whole lifecycle of the product. The risk assessment shall indicate the specific security requirements as set out in point 3 of section 1 of Annex I that are applicable to the respective product with digital elements and how these are implemented as informed by the risk assessment.	<u>comprise at least an analysis of (cybersecurity) risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use of the product with digital elements, such as the operational environment or the assets to be protected, (taking into account the whole lifecycle of the product). The cybersecurity risk assessment shall indicate if and how the security requirements set out in point 3 of Section 1 of Annex I are applicable to the respective product with digital elements and how these are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer will apply point 1 of Section 1 of the Annex I and the vulnerability handling requirements in Section 2 of Annex I.</u> LL to provide rewording on 'if and how' (also line 181). Alignment of support period/expected lifetime and cybersecurity risks. Issue of lifecycle to be solved later.
Article 10(3)				
181	3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the	3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the	3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the	3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.	technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.	technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.	technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation. Text Origin: Commission Proposal
Article 10(4)				
182	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~~ <u>It falls upon the manufacturer to</u> ensure that such components do not compromise the security of the product with digital elements, <u>including when integrating components of free and open-source software that have not been made available on the market in the course of a commercial activity.</u>	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 ~~in a manner~~ that such components do not compromise the security of the product with digital elements.	4. <u>EP COMP proposal:</u> 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~~ <u>a manner that such components do not compromise the cybersecurity of the product</u> with digital elements. ~~They shall ensure that such components do not compromise the security of,~~ <u>including when integrating components of free and open-source software that have not</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>Manufacturers shall, upon identifying a vulnerability in a component, including in a free and open-source component, which is integrated in the product with digital elements, address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Annex I, Section 2, and share the corrective measures taken with the person or entity maintaining the component.</u>	PUBLIC	<u>been made available on the market in the course of a commercial activity.</u> <u>Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is integrated in</u> the product with digital elements, <u>report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Annex I, Part 2.</u> <u>Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine readable format.</u> Merge of Article 10.4 and Article 11.7 (line 182 EP and line 204 Council) COM to provide COMP text in Article 10 Open source issue to be discussed later

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 10(4a)				
182a		<u>4a. The manufacturer of components shall provide to the manufacturer of the final product with digital elements the information and documentation necessary to comply with the requirements of this Regulation, when supplying them with such components. This information shall be provided free of charge.</u>		COM proposal to be included into Annex: Annex II (9) (e) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential requirements in Annex I as well as documentation requirements in Annex V of this Regulation.
Article 10(5)				
183	5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities they become aware of and any relevant information provided by third parties, and, where applicable, update the risk assessment of the product.	5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities they become aware of and any relevant information provided by third parties, and, where applicable, update the risk assessment of the product.	5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities ~~they become~~ it becomes aware of and any relevant information provided by third parties, and, where applicable, update the cybersecurity risk assessment of the product.	5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities ~~they become~~ it becomes aware of and any relevant information provided by third parties, and, where applicable, update the cybersecurity risk assessment of the product. Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 10(6), first subparagraph				
184	6. When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, 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.	6. When placing a product with digital elements on the market, <u>manufacturers shall determine the support period during which vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I. In doing so, the manufacturer shall ensure that the support period is proportionate to and for the expected product lifetime or for as well as in line with the nature of the product and users' expectations, the availability of the operating environment and, where applicable, the support period of five years from the placing of the the main components integrated into the product with digital elements. To that end manufacturers shall make available upon request of market surveillance authorities information on the expected product lifetime they considered in order to determine the duration of the support period for the product made available on the market, whichever is shorter, manufacturers. Market surveillance authorities shall monitor products with digital elements and ensure actively that manufacturers have applied these criteria in an adequate manner, including an</u>	6. Manufacturers shall ensure, when placing a product with digital elements on the market,– and for the expected product lifetime, that vulnerabilities of that– or for a period of five years from the placing of the product on the market, whichever is shorter, including its components, 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.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>assessment of the information received from the manufacturers on the expected ~~that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I~~ lifetime, when determining the support period.</u> <u>Where applicable, the support period shall be clearly stated on the product, its packaging or be included in contractual agreements. In any case, end users shall also be informed before purchase of the duration of the support period.</u>	PUBLIC	
Article 10(6), first subparagraph a				
184a			Manufacturers shall determine the expected product lifetime referred to in the first subparagraph of this paragraph taking into account the time users reasonably expect to be able to use the product with digital elements given its functionality and intended purpose and therefore can expect to receive security updates.	
Article 10(6), second subparagraph				
y 185	Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability	Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability	Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability	Partially covered by COM COMP y

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.	disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources. <u>Where applicable, for consumer products with digital elements, those procedures shall include automatic security updates by default. Users should retain the possibility of de-activating those automatic security updates.</u> <u>Manufacturers shall actively inform users when their product with digital elements has reached the end of its support period.</u>	disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.	EP check on placement and text of automatic security updates
Article 10(6a)				
Y	185a		Security updates, referred to in Section 2, point (8), of Annex I, which have been made available to users shall remain available for a minimum duration of 10 years.	Covered by COM COMP
Article 10(6b)				
Y	185b		6a. For the purpose of complying with the obligation provided for in the first subparagraph of paragraph 6, where manufacturers have placed	PRES/COM to provide rewording and explanatory recital

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			subsequent versions of a software product on the market, they may provide security updates only for the software product that they have last placed on the market. They may do so only if the users of the relevant previous product versions have access to the latest product version free of charge and do not incur significant additional costs to adjust the hardware and software environment in which they operate the product.	
Article 10(6c)				
185c		<u>6a. Where the support period is shorter than five years and the handling of vulnerabilities has ended, manufacturers may provide access to the source code of such a product with digital elements to other undertakings which commit to extending the provision of vulnerability handling services, in particular security updates. Access to such source codes shall be provided only where provided for in a contractual arrangement. Those arrangements shall protect the ownership of the product with digital elements and shall prevent the dissemination of the source code to the public, except where such code has already been provided under a free and open-</u>		Covered by COM COMP

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		source licence.		
	Article 10(6d)			
Y	185d		6b. This Regulation shall not prevent manufacturers from maintaining publicly available archives of previously made available software versions if they provide in a clear and easily accessible manner information on risks associated with using software that are not supported or updated anymore.	PRES to provide rewording and related recital - EP check
	Article 10(7), first subparagraph			
G	186	7. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23.	7. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23.	7. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23. Text Origin: Commission Proposal
	Article 10(7), second subparagraph			
G	187	They shall carry out the chosen conformity assessment procedures referred to in Article 24 or have them carried out.	They shall carry out the chosen conformity assessment procedures referred to in Article 24 or have them carried out.	They shall carry out the chosen conformity assessment procedures referred to in Article 24 or have them carried out. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 10(7), third subparagraph			
188	Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22.	Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22.	Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22.	Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22. Text Origin: Commission Proposal
	Article 10(8)			
189	8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.	8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, ~~where relevant,~~ at the disposal of the market surveillance authorities for <u>at least</u> ten years <u>or the support period, whichever is longer,</u> after the product with digital elements has been placed on the market. <u>Market surveillance authorities shall ensure the confidentiality and</u>	8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, ~~where relevant,~~ at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.	8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, ~~where relevant,~~ at the disposal of the market surveillance authorities for <u>at least</u> ten years <u>or the (support period/lifetime), whichever is longer,</u> after the product with digital elements has been placed on the market. <u>(Market surveillance authorities</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>appropriate protection of the information in the technical documentation provided by manufacturers in accordance with Article 52.</u>		<u>shall ensure the confidentiality and appropriate protection of the information in the technical documentation provided by manufacturers in accordance with Article 52.)</u> Align to lifetime/support period EP check (IMCO) on second paragraph Text Origin: EP Mandate
Article 10(9)				
190	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 <u>horizontal or sector specific</u> 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 with the requirements of this Regulation. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article ~~19~~18 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 <u>with the requirements of this Regulation</u>. 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~~18 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified. Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 10(9a)				
190a			9a. Manufacturers shall ensure that their products with digital elements bear a type, batch or serial number or other element allowing their identification, or, where that is not possible, on its packaging or in a document accompanying the product with digital elements.	<u>9a. Manufacturers shall ensure that their products with digital elements bear a type, batch or serial number or other element allowing their identification, or, where that is not possible, on its packaging or in a document accompanying the product with digital elements.</u> Text Origin: Council Mandate
Article 10(9aa)				
190b			9aa. Manufacturers shall indicate the name, registered trade name or registered trade mark of the manufacturer, and the postal address, email address or other digital contact as well as, where applicable, the website at which the manufacturer can be contacted, on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language which can be easily understood by users and market surveillance authorities.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 10(10)				
191	10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements.	10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements. <u>Where such information and instructions are provided in electronic form, manufacturers shall:</u> <u>(a) present them in a user-friendly format that makes it possible for the user to consult them online, download them, save them on an electronic device and print them;</u> <u>(b) ensure that they are accessible online during at least the support period of the product with digital elements.</u>	10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such information and instructions shall be provided in a language which can be easily understood by users and market surveillance authorities. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements.	
Article 10(10a)				
191a			10a. Manufacturers shall ensure that the end date for the expected product lifetime as referred to in	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			paragraph 6, including at least the month and year, until which the manufacturer will at least ensure the effective handling of vulnerabilities in accordance with the essential requirements set out in Section 2 of Annex I to this Regulation is clearly and understandably specified at the time of purchase, in an easily accessible manner and where applicable on the product with digital elements, its packaging or by digital means.	
Article 10(11)				
192	11. Manufacturers shall either provide the EU declaration of conformity with the product with digital elements or include in the instructions and information set out in Annex II the internet address at which the EU declaration of conformity can be accessed.	11. Manufacturers shall either provide the EU declaration of conformity with the product with digital elements or include in the instructions and information set out in Annex II the internet address at which the EU declaration of conformity can be accessed.	11. Manufacturers shall either provide a copy of the EU declaration of conformity or a simplified EU declaration of conformity with the product with digital elements. Where a simplified EU declaration of conformity is provided, it shall contain the exact ~~or include in the instructions and information set out in Annex II the internet address at which the~~ full EU declaration of conformity can be accessed.	
Article 10(12)				
193	12. From the placing on the market and for the expected product lifetime or for a period of five years after the	12. From the placing on the market and for ~~the expected product lifetime~~ ~~or for a~~ <u>at least the support</u> period ~~of~~	12. From the placing on the market and for the ~~expected product lifetime~~ ~~or for a period of five years after the~~	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	~~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.	~~placing on the market of a product with digital elements, whichever is shorter~~ time referred to in paragraph 6 , 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.	
Article 10(13)				
194	13. Manufacturers shall, further to a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by it, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in Annex I. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements, which	13. Manufacturers shall, further to a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by it, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in Annex I. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements, which	13. Manufacturers shall, further to a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by it, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in Annex I. They shall cooperate with that authority, at its request, on any measures taken to adequately reduce-eliminate the cybersecurity risks posed by the product with	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	they have placed on the market.	they have placed on the market.	digital elements, which they have placed on the market.	
Article 10(14)				
195	14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market.	14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market.	14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market.	14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market. Text Origin: Commission Proposal
Article 10(15)				
196	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, <u>after consulting the Expert Group and taking account of international standards, is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying</u> ~~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~~	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 and the format of the information and instructions referred to in Annex II . Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<i>adopted in accordance with the examination procedure referred to in Article 51(2).</i>		
Article 11				
197	Article 11 Reporting obligations of manufacturers	Article 11 Reporting obligations of manufacturers	Article 11 Reporting obligations of manufacturers	Article 11 Reporting obligations of manufacturers Text Origin: Commission Proposal
Article 11(1)				
198	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	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 in~~ <u>accordance with paragraph 1a of this Article</u> . 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]~~ <u>12</u> of Directive ~~[Directive XXX/XXXX - (NIS2 EU)]~~ <u>2022/2555</u>	1. The ~~manufacturer~~ manufacturers 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 that they become aware of to the CSIRT ~~CSIRTs~~ designated for the purposes of coordinated vulnerability disclosure in accordance with coordinators pursuant to Article [Article X] <u>12(1)</u>	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	surveillance authority about the notified vulnerability.	of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability. <u>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.</u>	of Directive ~~[Directive XXX/XXXX (NIS2 (EU))]~~ of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability. 2022/2555, in accordance with paragraph 2b of this Article.	
Article 11(1a)				
198a		<u>1a. Notifications as referred to in paragraph 1 shall be subject to the following procedure:</u>	1a. For the purpose of the notification referred to in paragraph 1, the manufacturers shall submit:	
Article 11(1a), point (a)				
198b		<u>(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the existence of an actively exploited vulnerability, including whether any known corrective or recommended risk mitigating measure is available;</u>	(a) Without undue delay and in any event within 24 hours of becoming aware of the actively exploited vulnerability, an early warning which shall provide general information, as available, about the product with digital elements concerned, the nature of the exploit and of the respective vulnerability. The early warning shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			product with digital elements has been made available. Where applicable, the early warning shall also indicate any corrective or mitigating measures taken, corrective or mitigating measures that users can take, and include an indication of how sensitive the manufacturer deems the notified information to be.	
Article 11(1a), point (b)				
198c		<u>(b) a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which, where applicable, updates the general information referred to in point (a), including any corrective or mitigating measures taken and indicates an assessment of extent of the vulnerability, including its severity and impact;</u>	(b) Without undue delay and in any event within 72 hours of becoming aware of the actively exploited vulnerability, a notification updating the information referred to in point (a). Where applicable, the notification shall indicate any available information about the actively exploited vulnerability, the status of remediation and any corrective or mitigating measures taken.	
Article 11(1a), point (c)				
198d		<u>(c) a final report, within one month after the submission of the vulnerability notification under point (b) or when a corrective or mitigating measure is available, including at least the following:</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 11(1a), point (c)(i)				
198e		<u>(i) a description of the vulnerability, including its severity and impact;</u>		
Article 11(1a), point (c)(ii)				
198f		<u>(ii) where available, information concerning any actor that has exploited or that is exploiting the vulnerability;</u>		
Article 11(1a), point (c)(iii)				
198g		<u>(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.</u>		
Article 11(1b)				
198h		<u>1b. After a security update is made available or another form of corrective or mitigating measures is put in place, ENISA shall add the notified vulnerability pursuant to paragraph 1 of this Article to the European vulnerability database referred to in Article 12 of Directive (EU) 2022/2555.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 11(2)				
199	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,~~ notify to ENISA any <u>significant</u> incident having impact on the security of the product with digital elements <u>in accordance with paragraph 2b of this Article</u>. 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]~~ <u>8</u> of Directive ~~[Directive XXX/XXXX (NIS2 EU)]~~ <u>2022/2555</u> of the Member States concerned and inform the market surveillance authority about the notified incidents. The ~~incident~~ <u>mere act of</u> notification shall ~~include information on the severity and impact of the~~ <u>not subject the notifying entity to increased liability</u>. <u>2a. An incident and shall be considered to be significant as referred to in paragraph 2,</u> where: <u>(a) it has caused or is capable of causing severe operational disruption of the production or the services for</u> ~~applicable, indicate whether~~ the manufacturer ~~suspects~~	2. The ~~manufacturer~~ manufacturers shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any incident having an 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 that they become aware of to the single point of contact CSIRTs designated in accordance with Article ~~[as coordinators pursuant to Article X]~~ 12(1) of Directive ~~[Directive XXX/XXXX (NIS2 EU)]~~ 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 2022/2555, in accordance with paragraph 2b of this Article.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		~~the incident to be caused by unlawful or malicious acts or considers it to have a cross-border~~ ~~impact~~concerned, which would impact the security of a product; or <u>(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.</u>		
Article 11(2a), first subparagraph				
199a			2b. The notifications referred to in paragraphs 1 and 2 shall be submitted through one of the electronic notification end-points of the single reporting platform referred to in paragraph 2c.	
Article 11(2a), second subparagraph				
199b			Where the manufacturers have their main establishment in the Union, they shall submit the notifications referred to in paragraphs 1 and 2 through the electronic notification end-point of the CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555 of the Member State in which they have their main establishment.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 11(2a), third subparagraph				
199c			For the purposes of this Regulation, a manufacturer shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken.	
Article 11(2a), fourth subparagraph				
199d			Where manufacturers have no main establishment in the Union, they shall notify via the single reporting platform to the CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555 in the Member State of their choice.	
Article 11(2b), first subparagraph				
199e			2c. For the purpose of the notifications referred to in paragraphs 1 and 2, a single reporting platform shall be established, and the day-to-day operations managed and maintained by ENISA. The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			end-points.	
Article 11(2b), second subparagraph				
199f			The initial recipient of a notification shall, without delay, disseminate the notification via the single reporting platform to all the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 on whose territory the manufacturer has indicated that the product with digital elements has been made available and to ENISA. In exceptional circumstances and in particular upon request by the manufacturer and in light of the level of sensitivity of the notified information as indicated by the manufacturer under paragraph 1a (a), the dissemination of the notification may be delayed based on justified cybersecurity related grounds for a period of time that is strictly necessary, including in cases where a vulnerability is subject to a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555. The CSIRTs network, established pursuant to Article 15 of Directive (EU) 2022/2555, shall adopt guidelines on the terms and	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			conditions for applying the aforementioned cybersecurity related grounds.	
Article 11(2b), third subparagraph				
199g			After receiving a notification regarding an actively exploited vulnerability in a product with digital elements or regarding an incident having an impact on the security of a product with digital elements, the CSIRTs shall provide market surveillance authorities of their respective Member States with the notified information necessary for the market surveillance authorities to fulfil their obligations under this Regulation.	
Article 11(2cc)				
199h			2cc. ENISA shall notify without undue delay any security incident affecting the single reporting platform to the CSIRTs network.	
Article 11(2d)				
199i			2d. The CSIRTs network shall provide specifications on the organisational matters regarding the establishment, maintenance	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			and secure operation of the single reporting platform, including at least the following:	
Article 11(2d), point (a)				
199j			(a) security arrangements related to the establishment, operation and maintenance of the platform, as well as the electronic notification end-points setup by the CSIRTs at national level, including security aspects;	
Article 11(2d), point (b)				
199k			(b) the type of information and format of the notifications.	
Article 11(2dd)				
199l			2dd. ENISA shall comply with the specifications provided by the CSIRTs network as referred to in paragraph 2d in the development and operations for the management and maintenance of the single reporting platform.	
Article 11(2aaaa)				
199m			2aaaa. Manufacturers of products with digital elements shall have	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			the possibility to voluntarily report vulnerabilities of which active exploitation has not yet been observed.	
Article 11(2aaaaa)				
199n			2aaaaa. Where a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555 has been made aware of an actively exploited vulnerability as part of a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555, the initial recipient CSIRT may delay the dissemination of the respective notification via the single reporting platform based on justified cybersecurity related grounds for a period of time that is strictly necessary and until consent for disclosure by the involved coordinated vulnerability disclosure-parties is reached. This does not prevent manufacturers from notifying such a vulnerability on a voluntary basis in accordance with the procedure laid down in this Article.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 11(2h)				
199o		<u>2b. Notifications as referred to in paragraph 2 shall be subject to the following procedure:</u>	2h. For the purpose of the notification referred to in paragraph 2, the manufacturers shall submit:	
Article 11(2h), point (a)				
199p		<u>(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the significant incident, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;</u>	(a) Without undue delay and in any event within 24 hours of becoming aware of the incident, an early warning which shall provide general information, as available, about the nature of the incident and shall indicate whether the incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact. The early warning shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available. Where applicable, the early warning shall also indicate any corrective or mitigating measures taken, corrective or mitigating measures that users can take, and include an indication of how sensitive the manufacturer deems the notified information to be.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 11(2h), point (b)				
199q		<u>(b) an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the significant incident, which, where applicable, shall update the information referred to in point (a) and indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;</u>	(b) Without undue delay and in any event within 72 hours of becoming aware of the incident, an incident notification which shall include information on the severity and impact of the incident, and, where applicable, update the information referred to in point (a). The notification shall also include, if available, information on the indicators of compromise.	
Article 11(2a), point (c)				
199r		<u>(c) a final report, within one month after the submission of the incident notification under point (b), including at least the following:</u>		
Article 11(2a), point (d)				
199s		<u>(i) a detailed description of the incident, including its severity and impact;</u>		
Article 11(2a), point (e)				
199t		<u>(ii) the type of threat or root cause that is likely to have triggered the incident;</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 11(2a), point (f)				
199u		<u>(iii) applied and ongoing mitigation measures;</u>		
Article 11(2a), point (g)				
199v		<u>(iv) where applicable, the cross-border impact of the incident;</u> <u>In the event of an ongoing incident at the time of the submission of the final report referred to in point (d) of this paragraph, Member States shall ensure that the manufacturer concerned provides a progress report at that time and a final report within one month of their handling of the incident.</u>		
Article 11(2a), point (i)				
199w		<u>2c. Manufacturers that have notified significant incidents according to this Regulation and that are also identified as essential entities or important entities under the Directive (EU) 2022/2555 shall be deemed compliant with the requirements under Article 23 of Directive (EU) 2022/2555. ENISA shall forward the notifications received pursuant to this Regulation to the responsible CSIRT according to Directive (EU)</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>2022/2555. An entity may only be fined once for non-compliance with overlapping requirements.</u>		
Article 11(2a), point (j)				
199x		<u>2d. Where necessary, ENISA or the relevant CSIRT may request manufacturers to provide an intermediate report on relevant status updates about the actively exploited vulnerability or significant incident.</u>		
Article 11(2a), point (k)				
199y		<u>2e. Manufacturers that qualify as microenterprises or as small or medium-sized enterprises shall be exempt from paragraph 1a, point (a) and paragraph 2b, point (a).</u>		
Article 11(2ab)				
199z			2ab. Where a third party other than the manufacturer notifies an actively exploited vulnerability or an incident having an impact on the security of a product with digital elements under the scope of this Regulation to a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555, that	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			CSIRT shall without undue delay inform the manufacturer.	
Article 11(3)				
200	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]~~ <u>16</u> of Directive ~~[Directive XXX/XXXX (NIS2)]~~ <u>2022/2555</u> 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~~ may submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by under Article ~~[Article X]~~ <u>16</u> of Directive ~~[Directive XXX/XXXX (NIS2)]~~ <u>2022/2555</u> information notified pursuant to paragraphs 1 (a), 1 (b), 2a (a) and 2a (b) ~~and 2~~ if such information is relevant for the coordinated management of ~~large-scale~~ large-scale cybersecurity incidents and crises at an operational level. For the purpose of determining such relevance, ENISA may consider technical analyses performed by the CSIRTs network, where available.	
Article 11(4)				
201	4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.	4. The manufacturer shall inform, without undue delay and after becoming aware, the impacted users of the product with digital elements, and where appropriate all users, about the significant incident and, where necessary, about risk mitigation and any corrective measures that the user can deploy to	4. The manufacturer shall inform, ~~without undue delay and~~ after becoming aware, the users of the product with digital elements about ~~the~~ an actively exploited vulnerability or an incident having an impact on the security of the product with digital elements and, where necessary, about corrective	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		mitigate the impact of the <u>significant</u> incident.	measures that the user can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured and easily automatically processible machine-readable format. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRT may provide such information to the users when considered proportionate and necessary for preventing or mitigating the impact of that vulnerability or the incident.	
Article 11(4a)				
201a		<u>4a. ENISA shall ensure that notifications pursuant to paragraphs 1 and 2 are submitted via channels of communication and stored on servers that ensure the highest possible levels of cybersecurity and protection from malicious actors.</u>		
Article 11(4b)				
201b		<u>4b. Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>incident is otherwise in the public interest, ENISA and, where appropriate, the CSIRTs or the competent authorities of the relevant Member States, may, after consulting the manufacturer concerned, inform the public about the significant incident or require the manufacturer to do so.</u>		
Article 11(5)				
202	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 ~~may, by means of implementing acts, specify further the type of information,~~ <u>shall adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying further the</u> format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those ~~implementing~~ <u>delegated</u> acts shall be adopted ~~in accordance with the examination procedure referred to in Article 51(2)~~ <u>by ... [12 months after the date of entry into force of this Regulation].</u>	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~~ <u>to 2ab of this Article</u> . Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	
Article 11(6)				
203	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	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	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	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article ~~[Article X]~~ 14 of Directive ~~[Directive XXX/XXXX (NIS2 EU)]~~ <u>2022/2555</u> . The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying. <u>ENISA shall include relevant information from its technical reports in its report on the state of cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555.</u>	cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in ~~in established under~~ Article ~~[Article X]~~ 14 of Directive ~~[Directive XXX/XXXX (NIS2 (EU))]~~ <u>2022/2555</u> . The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.	
Article 11(6a)				
203a		<u>6a. ENISA shall establish a secure digital reporting mechanism, after having consulted the Expert Group, in order to simplify reporting obligations of manufacturers. This mechanism shall serve as a single entry point for reporting obligations established under this Regulation and, where possible, other Union law.</u>		
Article 11(7)				
204	7. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is	<i>deleted</i>	7. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component.		integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component. Where manufacturers have developed a software modification to address the vulnerability in that component, they shall share the relevant code with the person or entity maintaining the component, where appropriate in a machine readable format.	
Article 11a				
204a		<u>Article 11a</u> <u>Voluntary notification</u>		
Article 11a(1)				
204b		<u>1. In addition to the notification obligations set out in Article 11, notifications may be submitted to ENISA on a voluntary basis by the following:</u>		
Article 11a(1), point (a)				
204c		<u>(a) manufacturers, with regard to incidents, cyber threats and near misses;</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 11a(1), point (b)				
204d		<u>(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Regulation, with regard to significant and non-significant incidents, cyber threats and near misses;</u>		
Article 11a(1), point (c)				
204e		<u>(c) any actor with regard to vulnerabilities which may be included in the European vulnerability database referred to in Article 12 of Directive 2022/2555.</u>		
Article 11a(2)				
204f		<u>2. ENISA shall process the notifications referred to in paragraph 1, point (a) of this Article in accordance with the procedure laid down in Article 11. ENISA may prioritise the processing of mandatory notifications over voluntary notifications.</u>		
Article 11a(3)				
204g		<u>3. In order to simplify the voluntary notifications, it shall be</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>possible to notify these through the secure digital reporting mechanism referred to in Article 11(6a).</u>		
Article 11a(4)				
204h		<u>4. Where appropriate, ENISA shall ensure the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.</u>		
Article 11a				
204i		<u>Article 11b</u> <u>Point of single contact for users</u>		EP will provide text to be included in Article 10
Article 11b(1)				
204j		<u>1. In order to facilitate reporting on the security of products, manufacturers shall designate a point of single contact to enable users to communicate directly and</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement	
		<u>rapidly with them, where applicable by electronic means and in a user-friendly manner, including by allowing users of the product to choose the means of communication set out in point 1 of Annex II, which shall not solely rely on automated tools.</u>	PUBLIC		
Article 11b(2)					
204k		<u>2. In addition to the obligations provided under Directive 2000/31/EC of the European Parliament and of the Council¹, manufacturers shall make public the information necessary for the end users in order to easily identify and communicate with their points of single contact. That information shall be easily accessible and shall be kept up to date.</u> <u>1. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).</u>			
Article 12					
205	Article 12 Authorised representatives	Article 12 Authorised representatives	Article 12 Authorised representatives	Article 12 Authorised representatives Text Origin: Commission	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Article 12(1)				
206	1. A manufacturer may appoint an authorised representative by a written mandate.	1. A manufacturer may appoint an authorised representative by a written mandate.	1. A manufacturer may ~~appoint an authorised representative~~ , by a written mandate, appoint an authorised representative .	1. A manufacturer may ~~appoint an authorised representative~~ , by a written mandate, <u>appoint an authorised representative</u> . Text Origin: Council Mandate
Article 12(2)				
207	2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.	2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.	2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.	2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate. Text Origin: Commission Proposal
Article 12(3)				
208	3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:	3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. <u>It shall provide a copy of the mandate to the market surveillance authorities upon request.</u> The mandate shall allow the authorised representative to do at least the following:	3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:	3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. <u>It shall provide a copy of the mandate to the market surveillance authorities upon request.</u> The mandate shall allow the authorised representative to do at least the following: Text Origin: EP Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 12(3), point (a)				
y	209	(a) keep the EU declaration of conformity referred to in Article 20 and the technical documentation referred to in Article 23 at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market;	(a) keep the EU declaration of conformity referred to in Article 20 and the technical documentation referred to in Article 23 at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market;	(a) keep the EU declaration of conformity referred to in Article 20 and the technical documentation referred to in Article 23 at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market; To be aligned with lifetime/support period Text Origin: Commission Proposal
Article 12(3), point (aa)				
y	209a	<u>(aa) where the authorised representative has a reason to believe that a product with digital elements in question presents a cybersecurity risk, inform the manufacturer;</u>		EP check
Article 12(3), point (b)				
g	210	(b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;	(b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;	(b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 12(3), point (c)				
211	(c) cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.	(c) cooperate with the market surveillance authorities, at their request, on any action taken to <u>effectively</u> eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.	(c) cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.	(c) cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate. Text Origin: Commission Proposal
Article 13				
212	Article 13 Obligations of importers	Article 13 Obligations of importers	Article 13 Obligations of importers	Article 13 Obligations of importers Text Origin: Commission Proposal
Article 13(1)				
213	1. Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.	1. Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.	1. Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.	1. Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 13(2), first subparagraph				
214	2. Before placing a product with digital elements on the market, importers shall ensure that:	2. Before placing a product with digital elements on the market, importers shall ensure that:	2. Before placing a product with digital elements on the market, importers shall ensure that:	2. Before placing a product with digital elements on the market, importers shall ensure that: Text Origin: Commission Proposal
Article 13(2), first subparagraph, point (a)				
215	(a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer;	(a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer;	(a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer;	(a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer; Text Origin: Commission Proposal
Article 13(2), first subparagraph, point (b)				
216	(b) the manufacturer has drawn up the technical documentation;	(b) the manufacturer has drawn up the technical documentation;	(b) the manufacturer has drawn up the technical documentation;	(b) the manufacturer has drawn up the technical documentation; Text Origin: Commission Proposal
Article 13(2), first subparagraph, point (c)				
217	(c) the product with digital elements bears the CE marking referred to in Article 22 and is accompanied by the	(c) the product with digital elements bears the CE marking referred to in Article 22, <u>the EU declaration of</u>	(c) the product with digital elements bears the CE marking referred to in Article 22 and is accompanied by the	(c) the product with digital elements bears the CE marking referred to in Article 22 and is accompanied by the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	information and instructions for use as set out in Annex II.	<u>conformity is available and the product</u> ~~and~~ is accompanied by the information and instructions for use as set out in Annex II.	required documents as referred to in Article 10(11) and the information and instructions for use as set out in Annex II in a language which can be easily understood by users and market surveillance authorities.	<u>EU declaration of conformity as referred to in Article 10(11) and the information and instructions for use as set out in Annex II</u> <u>in a language which can be easily understood by users and market surveillance authorities.</u> Text Origin: Council Mandate
Article 13(2), first subparagraph, point (ca)				
Y	217a		(d) The manufacturer has complied with the requirements set out in Article 10(9a), 10(9aa) and 10(10a).	<u>(d) The manufacturer has complied with the requirements set out in Article 10(9a), 10(9aa) and 10(10a).</u> To be checked against Article 10. Text Origin: Council Mandate
Article 13(2), second subparagraph				
G	217b	<u>(ca) all the documents proving the fulfilment of the requirements set out in this Article have been received from the manufacturer.</u>		<u>For the purposes of this paragraph, importers shall be able to provide the necessary documents proving the fulfilment of the requirements set out in this Article.</u> Text Origin: EP Mandate
Article 13(3)				
Y	218	3. Where an importer considers or has reason to believe that a product	3. Where an importer considers or has reason to believe that a product	To be dealt with together with Articles

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.	with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect. <u>On the basis of targeted recommendations received by market surveillance authorities or by the Commission in accordance with Articles 43 and 45, an importer shall apply such recommendations, including withdrawing or recalling the product. Additionally, where an importer considers or has reasons to believe that a product with digital elements may present a cybersecurity risk in light of non-technical risk factors, it shall withdraw or recall that product. Importers shall inform the market surveillance authorities and the Commission to that effect.</u>	with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.	41, 43 and 45. In first subparagraph, change 'Annex I' to 'this Regulation'.
Article 13(4)				

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
219	4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and the email address at which they can be contacted on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.	4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and the email address, <u>and where available, the website</u> , at which they can be contacted on the product with digital elements or, ~~where that is not possible,~~ on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.	4. Importers shall indicate their name, registered trade name or registered trademark, the postal address, email address or other digital contact as well as, where applicable, the website and the email address at which they can be contacted on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.	4. Importers shall indicate their name, registered trade name or registered trademark, the postal address, <u>email address or other digital contact as well as, where applicable, the website</u> and the ~~email address~~ at which they can be contacted on the product with digital elements or, ~~where that is not possible,~~ on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities. Text Origin: Council Mandate
Article 13(5)				
220	5. Importers shall ensure that the product with digital elements is accompanied by the instructions and information set out in Annex II in a language which can be easily understood by users.	5. Importers shall ensure that the product with digital elements is accompanied by the instructions and information set out in Annex II in a language which can be easily understood by users.	<i>deleted</i>	5. ~~Importers shall ensure that the product with digital elements is accompanied by the instructions and information set out in Annex II in a language which can be easily understood by users.~~ Text Origin: Commission Proposal
Article 13(6), first subparagraph				
221	6. Importers who know or have reason to believe that a product with digital elements, which they have	6. Importers who know or have reason to believe that a product with digital elements, which they have	6. Importers who know or have reason to believe that a product with digital elements, which they have	6. Importers who know or have reason to believe that a product with digital elements, which they have

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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 <u>request the manufacturer to</u> 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.	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.	placed on the market, ~~or the processes put in place by its manufacturer, are~~ <u>is</u> not in conformity with ~~the essential requirements set out in Annex I~~ <u>this Regulation</u> shall immediately take the corrective measures necessary to ~~bring that~~ <u>ensure that the</u> product with digital elements ~~or the processes put in place by its manufacturer~~ <u>is brought</u> into conformity ~~with the essential requirements set out in Annex I~~ , or to withdraw or recall the product, if appropriate. to be aligned throughout text Text Origin: EP Mandate
Article 13(6), second subparagraph				
222	Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they made the product with digital elements available on the market to that effect, giving details, in	Upon ~~identifying~~ <u>becoming aware of</u> a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they made the product with digital elements available on the market to that effect, giving details, in	Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they made the product with digital elements available on the market to that effect, giving details, in	Upon ~~identifying~~ <u>becoming aware of</u> a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they made the product with digital elements available on the market to that effect, giving details, in

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	particular, of the non-conformity and of any corrective measures taken.	particular, of the non-conformity and of any corrective measures taken.	particular, of the non-conformity and of any corrective measures taken.	particular, of the non-conformity and of any corrective measures taken. Text Origin: EP Mandate
Article 13(7)				
223	7. Importers shall, for ten years after the product with digital elements has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.	7. Importers shall, for ten years after the product with digital elements has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.	7. Importers shall, for ten years after the product with digital elements has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.	7. Importers shall, for ten years after the product with digital elements has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request. to be aligned with Article 10 Text Origin: Commission Proposal
Article 13(8)				
224	8. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the	8. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the	8. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the	8. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.	manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.	manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any ~~measures~~ action taken to ~~adequately reduce~~ eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.	manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market. Text Origin: Commission Proposal
Article 13(9)				
225	9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.	9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.	9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.	9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market. Text Origin: Commission Proposal
Article 14				
226	Article 14	Article 14	Article 14	Article 14

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Obligations of distributors	Obligations of distributors	Obligations of distributors	Obligations of distributors Text Origin: Commission Proposal
Article 14(1)				
227	1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements of this Regulation.	1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements of this Regulation.	1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements of this Regulation.	1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements of this Regulation. Text Origin: Commission Proposal
Article 14(2)				
228	2. Before making a product with digital elements available on the market, distributors shall verify that:	2. Before making a product with digital elements available on the market, distributors shall verify that:	2. Before making a product with digital elements available on the market, distributors shall verify that:	2. Before making a product with digital elements available on the market, distributors shall verify that: Text Origin: Commission Proposal
Article 14(2), point (a)				
229	(a) the product with digital elements bears the CE marking;	(a) the product with digital elements bears the CE marking;	(a) the product with digital elements bears the CE marking;	(a) the product with digital elements bears the CE marking; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 14(2), point (b)			
230	(b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), 10(11) and 13(4).	(b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), 10(11) and 13(4), <u>and have communicated all relevant documents to the distributor.</u>	(b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(9a), 10 (9aa), 10(10), 10(10a+0), 10(11) and 13(4).	(b) the manufacturer and the importer have complied with the obligations set out respectively in Articles <u>10(9a), 10 (9aa), 10(10), 10(10a), 10(11) and 13(4)</u> <u>and have communicated all necessary documents to the distributor.</u> Text in () to be aligned with Article 10 Text Origin: Council Mandate
	Article 14(3)			
231	3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.	3. Where a distributor considers or has reason to believe, <u>on the basis of information in its possession</u> , that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.	3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform without undue delay the manufacturer and the market surveillance authorities to that effect.	3. Where a distributor considers or has reason to believe, <u>on the basis of information in its possession</u> , that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform <u>without undue delay</u> the manufacturer and the market surveillance authorities to that effect.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: EP Mandate
Article 14(4), first subparagraph				
232	4. Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.	4. Distributors who know or have reason to believe, <u>on the basis of information in their possession</u> , that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall ~~make sure that the~~ <u>request the manufacturer to take</u> corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.	4. Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.	4. Distributors who know or have reason to believe, <u>on the basis of information in their possession</u> , that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with ~~the essential requirements set out in Annex I~~ <u>this Regulation</u> shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate. To be aligned throughout text
Article 14(4), second subparagraph				
233	Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance	Upon ~~identifying~~ <u>becoming aware of</u> a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance	Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance	Upon ~~identifying~~ <u>becoming aware of</u> a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.	authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.	authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.	authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken. Text Origin: EP Mandate

Article 14(5)

234	5. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market.	5. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market.	5. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market.	5. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with ~~the essential requirements set out in Annex I~~ <u>this Regulation</u> in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market. Text Origin: Commission Proposal

Article 14(6)

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
G	235	6. <u>On the basis of information in its possession</u> , when the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.	6. When the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform, without undue delay , the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.	6. When the distributor of a product with digital elements becomes aware, <u>on the basis of information in its possession</u> , that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform, <u>without undue delay</u> , the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.
	Article 15			
G	236	Article 15 Cases in which obligations of manufacturers apply to importers and distributors	Article 15 Cases in which obligations of manufacturers apply to importers and distributors	Article 15 Cases in which obligations of manufacturers apply to importers and distributors Text Origin: Commission Proposal
	Article 15, first paragraph			
Y	237	An importer or distributor shall be considered a manufacturer for the purposes of this Regulation and shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7) where that	An importer or distributor shall be considered a manufacturer for the purposes of this Regulation and shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (1a), (2), (2a), (2b) ,	An importer or distributor shall be considered a manufacturer for the purposes of this Regulation and shall be subject to ~~the obligations of the manufacturer set out in~~ Articles 10 and 11(1), <u>(1a), (2), (2a), (2b)</u> ,

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	importer or distributor places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements already placed on the market.	importer or distributor places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements already placed on the market.	2(aaaa)(2), (4) and (7) where that importer or distributor places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements already placed on the market.	2(aaaa)(2), (4) and (7) where that importer or distributor places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements already placed on the market. To be aligned with Article 10/11/11a Text Origin: Council Mandate
Article 16				
238	Article 16 Other cases in which obligations of manufacturers apply	Article 16 Other cases in which obligations of manufacturers apply	Article 16 Other cases in which obligations of manufacturers apply	Article 16 Other cases in which obligations of manufacturers apply Text Origin: Commission Proposal
Article 16, first paragraph				
239	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 <u>and makes it available on the market</u> , 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 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 <u>and makes it available on the market</u> , shall be considered a manufacturer for the purposes of this Regulation. Text Origin: EP Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 16, second paragraph				
240	That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.	That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.	That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (1a), (2), (2a), (2b), 2(aaaa), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.	That person shall be subject to ~~the obligations of the manufacturer set out in~~ Articles 10 and 11(1), (1a), (2), (2a), (2b), 2(aaaa), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product. To be aligned with Article 10/11/11a Text Origin: Council Mandate
Article 17				
241	Article 17 Identification of economic operators	Article 17 Identification of economic operators	Article 17 Identification of economic operators	Article 17 Identification of economic operators Text Origin: Commission Proposal
Article 17(1)				
242	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 ~~and where the information is available~~ , provide to the market surveillance authorities the following information:	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 ~~and where the information is available~~ , provide to the market surveillance authorities the following information: Text Origin: EP Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 17(1), point (a)				
243	(a) name and address of any economic operator who has supplied them with a product with digital elements;	(a) name and address of any economic operator who has supplied them with a product with digital elements;	(a) name and address of any economic operator who has supplied them with a product with digital elements;	(a) name and address of any economic operator who has supplied them with a product with digital elements; Text Origin: Commission Proposal
Article 17(1), point (b)				
244	(b) name and address of any economic operator to whom they have supplied a product with digital elements;	(b) name and address of any economic operator to whom they have supplied a product with digital elements;	(b) name and address of any economic operator to whom they have supplied a product with digital elements;	(b) name and address of any economic operator to whom they have supplied a product with digital elements, <u>where the information is available</u> ; Text Origin: Commission Proposal
Article 17(2)				
245	2. Economic operators shall be able to present the information referred to in paragraph 1 for ten years after they have been supplied with the product with digital elements and for ten years after they have supplied the product with digital elements.	2. Economic operators shall be able to present the information referred to in paragraph 1 for ten years after they have been supplied with the product with digital elements and for ten years after they have supplied the product with digital elements.	2. Economic operators shall be able to present the information referred to in paragraph 1 for ten years after they have been supplied with the product with digital elements and for ten years after they have supplied the product with digital elements.	2. Economic operators shall be able to present the information referred to in paragraph 1 for ten years after they have been supplied with the product with digital elements and for ten years after they have supplied the product with digital elements. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 17a				
245a		<u>Article 17a Guidelines</u>		Council check
Article 17a(1)				
245b		<u>1. In order to create clarity, certainty for, and consistency among the practices of economic operators, the Commission shall prepare and issue guidelines for economic operators, explaining how to apply this Regulation, with a particular focus on how to facilitate compliance by microenterprises, small enterprises and medium-sized enterprises.</u>		
Article 17a(2)				
245c		<u>2. The guidelines shall be published by ... [12 months after the date of entry into force of this Regulation] and shall be updated as necessary, in particular in light of potential amendments to the list of critical products set out in Annex III. They shall contain at least the following elements:</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 17a(2), point (a)				
245d		<u>(a) a detailed explanation of the scope of this Regulation, with a particular focus on remote data processing solutions and free and open-source software;</u>		
Article 17a(2), point (b)				
245e		<u>(b) detailed criteria used to determine how critical products with digital elements are placed in classes I or II as set out in Annex III;</u>		
Article 17a(2), point (c)				
245f		<u>(c) the interplay between this Regulation and other Union law, particularly concerning presumptions of conformity and conformity assessments;</u>		
Article 17a(2), point (d)				
245g		<u>(d) guidance for manufacturers on how to perform the cybersecurity risk assessment referred to in Article 10(2) and on the applicability of the essential requirements including where available best practices;</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 17a(2), point (e)				
245h		<u>(e) guidance for manufacturers on how to determine appropriately the support period for different product categories in accordance with Article 10(6);</u>		
Article 17a(2), point (f)				
245i		<u>(f) an explanation of how to handle reporting requirements pursuant to this Regulation or other Union law;</u>		
Article 17a(2), point (g)				
245j		<u>(g) a list of the delegated and implementing acts published by the Commission pursuant to this Regulation;</u>		
Article 17a(2), point (h)				
245k		<u>(h) guidance for Member States on the non-prosecution of information security researchers;</u>		
Article 17a(2), point (i)				
245l		<u>(i) guidance on what constitutes substantial modifications.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 17a(3)				
245m		<u>3. When preparing the guidelines pursuant to this Article, the Commission shall consult the Expert Group.</u>		
CHAPTER III				
246	CHAPTER III Conformity of the product with digital elements	CHAPTER III Conformity of the product with digital elements	CHAPTER III Conformity of the product with digital elements	CHAPTER III Conformity of the product with digital elements Text Origin: Commission Proposal
Article 18				
247	Article 18 Presumption of conformity	Article 18 Presumption of conformity	Article 18 Presumption of conformity	Article 18 Presumption of conformity Text Origin: Commission Proposal
Article 18(1)				
248	1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with	1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with	1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with	1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	the essential requirements covered by those standards or parts thereof, set out in Annex I.	the essential requirements covered by those standards or parts thereof, set out in Annex I. <u>The Commission shall in accordance with Article 10(1) of Regulation (EU) 1025/2012 request one or more European standardisation organisations to draft harmonised standards for the essential requirements set out in Annex I to this Regulation. When preparing the standardisation request for this Regulation, the Commission shall strive to take into account existing or imminent international standards for cybersecurity in order to simplify the development of harmonised standards.</u>	the essential requirements set out in Annex I covered by those standards or parts thereof, ~~set out in Annex I.~~	the essential requirements <u>set out in Annex I</u> covered by those standards or parts thereof. <u>The Commission shall in accordance with Article 10(1) of Regulation (EU) 1025/2012 request one or more European standardisation organisations to draft harmonised standards for the essential requirements set out in Annex I to this Regulation. (When preparing the standardisation request for this Regulation, the Commission shall strive to take into account existing or imminent international standards for cybersecurity in order to simplify the development of harmonised standards.)</u> COM to provide COMP on text in () including "European and international existing and imminent standards" Text Origin: EP Mandate
Article 18(2)				
249	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	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	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 Commission	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~~

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	requirements set out in Annex I, to the extent those common specifications cover those requirements.	requirements set out in Annex I, to the extent those common specifications cover those requirements.	shall, as provided in Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the essential requirements set out in Annex I, ~~to the extent those common specifications cover those requirements.~~	~~requirements set out in Annex I, to the extent those common specifications cover those requirements.~~ Text Origin: Commission Proposal
Article 18(2a), first subparagraph				
249a			3. The Commission may adopt implementing acts establishing common specifications covering technical requirements that provide a means to comply with the essential requirements set out in Annex I for products with digital elements within the scope of this Regulation.	<u>3. The Commission may adopt (delegated/implementing acts) establishing common specifications covering technical requirements that provide a means to comply with the essential requirements set out in Annex I for products with digital elements within the scope of this Regulation.</u> D/IA issue Text Origin: Council Mandate
Article 18(2a), second subparagraph				
249b			Those implementing acts shall only be adopted where the following conditions are fulfilled:	<u>Those (delegated/implementing acts) shall only be adopted where the following conditions are fulfilled:</u> D/IA issue Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 18(2a), second subparagraph, point (a)			
249c			(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:	<u>(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:</u> Text Origin: Council Mandate
	Article 18(2a), second subparagraph, point (a)(i)			
249d			(i) the request has not been accepted; or	<u>(i) the request has not been accepted; or</u> Text Origin: Council Mandate
	Article 18(2a), second subparagraph, point (a)(ii)			
249e			(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or	<u>(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or</u> Text Origin: Council Mandate
	Article 18(2a), second subparagraph, point (a)(iii)			
249f			(iii) the harmonised standards do	<u>(iii) the harmonised standards do</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			not comply with the request; and	<u>not comply with the request; and</u> Text Origin: Council Mandate
Article 18(2a), second subparagraph, point (a)(iv)				
G	249g		(b) no reference to harmonised standards covering the relevant essential requirements set out in Annex I has been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.	<u>(b) no reference to harmonised standards covering the relevant essential requirements set out in Annex I has been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.</u> Text Origin: Council Mandate
Article 18(2b)				
Y	249h		Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	D/IA issue
Article 18(2c)				
Y	249i		4. Before preparing the draft implementing act referred to in paragraph 3, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers that the	D/IA issue. See also line 253c (expert group)

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			conditions in paragraph 3 have been fulfilled.	
	Article 18(2d)			
249j			5. When preparing the draft implementing act referred to in paragraph 3, the Commission shall take into account the views of relevant bodies or the expert group and shall duly consult all relevant stakeholders.	D/IA issue. See also line 253c (expert group)
	Article 18(2e)			
249k			6. Products with digital elements and processes put in place by the manufacturer which are in conformity with the common specifications established by implementing acts referred to in paragraph 3, or parts thereof, shall be presumed to be in conformity with the essential requirements set out in Annex I covered by those common specifications or parts thereof . Text largely based on Article 18(2) of the Commission proposal.	<u>6. Products with digital elements and processes put in place by the manufacturer which are in conformity with the common specifications established by (delegated/implementing acts) referred to in paragraph 3, or parts thereof, shall be presumed to be in conformity with the essential requirements set out in Annex I covered by those common specifications or parts thereof.</u> D/IA issue Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 18(2f)				
249l			7. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the implementing acts referred to in paragraph 3, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.	<u>7. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the (delegated/implementing acts) referred to in paragraph 3, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.</u> D/IA issue Text Origin: Council Mandate
Article 18(2g)				
249m			8. When a Member State considers that a common specification does not entirely satisfy the essential requirements set out in Annex I, it shall inform the Commission thereof by submitting a detailed explanation.	<u>8. When a Member State considers that a common specification does not entirely satisfy the essential requirements set out in Annex I, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.	<u>assess that detailed explanation and may, if appropriate, amend the (delegated/implementing act) establishing the common specification in question.</u> D/IA issue Text Origin: Council Mandate
Article 18(3)				
250	3. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 and specified as per paragraph 4, shall be presumed to be in conformity with the essential requirements set out in Annex I in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.	3. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 and specified as per paragraph 4, shall be presumed to be in conformity with the essential requirements set out in Annex I in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.	39. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 ~~and specified as per paragraph 4~~ , shall be presumed to be in conformity with the essential requirements set out in Annex I ~~in so far as the EU statement and related~~ conformity assessment procedures . For the purposes of the presumption of conformity, products with digital elements that need to undergo the conformity assessment procedures referred to in Article 24 (2) and (3) shall have a European cybersecurity certificate, or parts thereof, cover those requirements that refers to the required assurance level.	3. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 ~~and specified as per paragraph 4~~ , shall be presumed to be in conformity with the essential requirements set out in Annex I in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 18(4)				
251	4. The Commission is empowered, by means of implementing acts, to specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I. Furthermore, where applicable, the Commission shall specify if a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	4. The Commission is empowered <u>to adopt</u>, by means of ~~implementing acts, to specify~~ <u>delegated acts in accordance with Article 50, to supplement this Regulation by specifying</u> the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity <u>of products with digital elements</u> with the essential requirements or parts thereof as set out in Annex I. Furthermore, ~~where applicable, the Commission shall specify if the~~ <u>issuance of</u> a cybersecurity certificate issued under such schemes, <u>at assurance level 'substantial' or 'high'</u>, 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).~~	410. The Commission is empowered ~~may~~, 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~~ <u>cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party and related conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b) procedures.</u> Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	4. The Commission <u>(is empowered/may) to adopt</u> ~~is empowered~~, by means of ~~implementing acts, to specify~~ <u>(delegated/implementing acts in accordance with Article 50), to supplement this Regulation by specifying</u> the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity <u>of products with digital elements</u> with the essential requirements or parts thereof as set out in Annex I. Furthermore, ~~where applicable, the Commission shall specify if the~~ <u>issuance of</u> a cybersecurity certificate issued under such schemes, <u>(at required/assurance level 'substantial' or 'high',)</u> 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).~~ D/IA issue EP and Council check: assurance level Text Origin: EP Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 19				
252	Article 19 Common specifications	Article 19 Common specifications	deleted	deleted EP text included into Article 18
Article 19, first paragraph				
253	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).	<u>1. 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</u> <u>is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by establishing common specifications that cover technical requirements providing a means of implementing acts, to adopt common specifications in respect of the essential</u> <u>to comply with the</u> requirements set out in Annex I-	deleted	deleted

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<i>Those implementing acts shall be adopted in accordance with the examination procedure referred to in ~~Article 51(2)~~ for products that fall within the scope of this Regulation where the following conditions have been fulfilled:</i>		
Article 19, 1., point (a)				
253a		<i>(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 the request has not been accepted or the European standardisation deliverables addressing that request is not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012 or European standardisation deliverables do not comply with the request; and</i>		
Article 19, 1., point (b)				
253b		<i>(b) no reference to harmonised standards covering the relevant essential requirements set out in Annex I to this Regulation is published in the Official Journal of the European Union in accordance</i>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.</u>		
Article 19(2)				
G	253c	<u>2. Before preparing the delegated act, the Commission shall inform the Expert Group that it considers that the conditions in paragraph 1 are fulfilled. In preparing the delegated acts, the Commission shall take into account the opinions of the Expert Group.</u>		G
Article 19(3)				
G	253d	<u>3. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the publication of its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference to a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the relevant delegated acts referred to in paragraph 1, or the parts thereof which cover the same essential requirements set out</u>		G

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>in Annex I to this Regulation.</u>		
Article 20				
254	Article 20 EU declaration of conformity	Article 20 EU declaration of conformity	Article 20 EU declaration of conformity	Article 20 EU declaration of conformity Text Origin: Commission Proposal
Article 20(1)				
255	1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 10(7) and state that the fulfilment of the applicable essential requirements set out in Annex I has been demonstrated.	1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 10(7) and state that the fulfilment of the applicable essential requirements set out in Annex I has been demonstrated.	1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 10(7) and state that the fulfilment of the applicable essential requirements set out in Annex I has been demonstrated.	1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 10(7) and state that the fulfilment of the applicable essential requirements set out in Annex I has been demonstrated. Text Origin: Commission Proposal
Article 20(1a)(2)				
256	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	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~~ <u>updated as appropriate</u> . It shall be made available in the language or languages required by	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	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~~ <u>updated as appropriate</u> . It shall be made available in the language or languages required by

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	which the product with digital elements is placed on the market or made available.	the Member State in which the product with digital elements is placed on the market or made available.	which the product with digital elements is placed on the market or made available on the market .	the Member State in which the product with digital elements is placed on the market or made available <u>on the market</u> . Text Origin: EP Mandate
Article 20(1a), (2) a				
256a			The simplified EU declaration of conformity referred to in Article 10(11) shall contain the model structure set out in Annex [XX] and shall be continuously updated. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market. The full text of the EU declaration of conformity shall be available at the internet address referred to in the simplified EU declaration of conformity, in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market.	<u>The simplified EU declaration of conformity referred to in Article 10(11) shall contain the model structure set out in Annex [XX] and shall be continuously updated. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market. The full text of the EU declaration of conformity shall be available at the internet address referred to in the simplified EU declaration of conformity, in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market.</u> To be aligned with Article 10(11) Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 20(3)				
257	3. Where a product with digital elements is subject to more than one Union act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union acts. That declaration shall contain the identification of the Union acts concerned, including their publication references.	3. Where a product with digital elements is subject to more than one Union act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union acts. That declaration shall contain the identification of the Union acts concerned, including their publication references.	3. Where a product with digital elements is subject to more than one Union act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union acts. That declaration shall contain the identification of the Union acts concerned, including their publication references.	3. Where a product with digital elements is subject to more than one Union act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union acts. That declaration shall contain the identification of the Union acts concerned, including their publication references. Text Origin: Commission Proposal
Article 20(4)				
258	4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product.	4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product.	4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product.	4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product. Text Origin: Commission Proposal
Article 20(5)				
259	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by adding elements to the minimum content of the EU declaration of conformity set out in Annex IV to	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by adding elements to the minimum content of the EU declaration of conformity set out in Annex IV to	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by adding elements to the minimum content of the EU declaration of conformity set out in Annex IV to	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by adding elements to the minimum content of the EU declaration of conformity set out in Annex IV to

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	take account of technological developments.	take account of technological developments.	take account of technological developments.	take account of technological developments. Text Origin: Commission Proposal
Article 21				
260	Article 21 General principles of the CE marking	Article 21 General principles of the CE marking	Article 21 General principles of the CE marking	Article 21 General principles of the CE marking Text Origin: Commission Proposal
Article 21, first paragraph				
261	The CE marking as defined in Article 3(32) shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.	The CE marking as defined in Article 3(32) shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.	The CE marking as defined in Article 3(32) shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.	The CE marking as defined in Article 3(32) shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008. Text Origin: Commission Proposal
Article 22				
262	Article 22 Rules and conditions for affixing the CE marking	Article 22 Rules and conditions for affixing the CE marking	Article 22 Rules and conditions for affixing the CE marking	Article 22 Rules and conditions for affixing the CE marking Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 22(1)				
263	1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 20 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product.	1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 20 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product. <u>In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.</u>	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 packaging. and where applicable to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product packaging.	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. <u>In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.</u> Text Origin: EP Mandate
Article 22(2)				
264	2. On account of the nature of the product with digital elements, the height of the CE marking affixed to the product with digital elements may be lower than 5 mm, provided that it remains visible and legible.	2. On account of the nature of the product with digital elements, the height of the CE marking affixed to the product with digital elements may be lower than 5 mm, provided that it remains visible and legible.	2. On account of the nature of the product with digital elements, the height of the CE marking affixed to the product with digital elements may be lower than 5 mm, provided that it remains visible and legible.	2. On account of the nature of the product with digital elements, the height of the CE marking affixed to the product with digital elements may be lower than 5 mm, provided that it remains visible and legible. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 22(3)			
265	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 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 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 a special risk or use set out in implementing acts referred to in paragraph 6. Text Origin: Commission Proposal
	Article 22(4), first subparagraph			
266	4. The CE marking shall be followed by the identification number of the notified body, where that body is involved in the conformity assessment procedure based on full quality assurance (based on module H) referred to in Article 24.	4. The CE marking shall be followed by the identification number of the notified body, where that body is involved in the conformity assessment procedure based on full quality assurance (based on module H) referred to in Article 24.	4. The CE marking shall be followed by the identification number of the notified body, where that body is involved in the conformity assessment procedure based on full quality assurance (based on module H) referred to in Article 24.	4. The CE marking shall be followed by the identification number of the notified body, where that body is involved in the conformity assessment procedure based on full quality assurance (based on module H) referred to in Article 24. Text Origin: Commission Proposal
	Article 22(4), second subparagraph			
267	The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised	The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised	The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised	The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	representative.	representative.	representative.	representative. Text Origin: Commission Proposal
Article 22(5)				
268	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.	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.	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.	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. Text Origin: Commission Proposal
Article 22(6)				
269	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	6. <u>After consulting the Expert Group, the dedicated administrative cooperation group (ADCO) and, where necessary, other relevant stakeholders</u> , the Commission may, by means of implementing acts, lay down technical specifications for <u>labelling schemes, including harmonised labels</u> , pictograms or any other marks related to the	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	6. <u>(After consulting the Expert Group, the dedicated administrative cooperation group (ADCO) and, where necessary, other relevant stakeholders)</u> , the Commission may, by means of implementing acts, lay down technical specifications for <u>labels</u> , pictograms or any other marks related to the security of the products with digital elements, <u>their</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 51(2).	security of the products with digital elements, <u>their support period</u> and mechanisms to promote their use <u>among businesses and consumers and to increase public awareness about the security of products with digital elements</u> . Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	Article 51(2).	<u>(lifetime/support period)</u> and mechanisms to promote their use <u>and to increase public awareness about the security of products with digital elements</u> . Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2). To be aligned with EP Article 6a (expert group) and EP to up-date text in (). To be aligned with Article 10(6) (lifetime/support period). Text Origin: EP Mandate
Article 23				
270	Article 23 Technical documentation	Article 23 Technical documentation	Article 23 Technical documentation	Article 23 Technical documentation Text Origin: Commission Proposal
Article 23(1)				
271	1. The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential requirements set out in Annex I. It shall at least contain the	1. The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential requirements set out in Annex I. It shall at least contain the	1. The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential requirements set out in Annex I. It shall at least contain the	1. The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential requirements set out in Annex I. It shall at least contain the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	elements set out in Annex V.	elements set out in Annex V.	elements set out in Annex V.	elements set out in Annex V. Text Origin: Commission Proposal
Article 23(2)				
272	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~~ <u>during at least the support period of five years after the placing on the market of a product with digital elements, whichever is shorter.</u>	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~~ <u>during a period of five years after the placing on the market of a product with digital elements, whichever is shorter at least the (support period/lifetime).</u> To be aligned with Article 10(6) Text Origin: EP Mandate
Article 23(3)				
273	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 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 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 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. Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Article 23(4)				
274	4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body.	4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body.	4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body.	4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body. Text Origin: Commission Proposal
Article 23(5)				
275	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. <u>The Commission shall ensure that the administrative burden on microenterprises and small and medium-sized enterprises is proportionate.</u>	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. <u>For this purpose, the Commission shall strive to ensure that the administrative burden on microenterprises and small and medium-sized enterprises is proportionate.</u> Text Origin: EP Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 24				
276	Article 24 Conformity assessment procedures for products with digital elements	Article 24 Conformity assessment procedures for products with digital elements	Article 24 Conformity assessment procedures for products with digital elements	Article 24 Conformity assessment procedures for products with digital elements Text Origin: Commission Proposal
Article 24(1)				
277	1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements by using one of the following procedures:	1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements by using one of the following procedures:	1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer ~~or the manufacturer's authorised representative~~ shall demonstrate conformity with the essential requirements by using ~~one~~ any of the following procedures:	1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer ~~or the manufacturer's authorised representative~~ shall demonstrate conformity with the essential requirements by using ~~one~~ any of the following procedures: Text Origin: Council Mandate
Article 24(1), point (a)				
278	(a) the internal control procedure (based on module A) set out in Annex VI; or	(a) the internal control procedure (based on module A) set out in Annex VI; or	(a) the internal control procedure (based on module A) set out in Annex VI; ~~or~~	(a) the internal control procedure (based on module A) set out in Annex VI; ~~or~~ Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 24(1), point (b)				
279	(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	(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	(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	(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~~ Text Origin: Council Mandate
Article 24(1), point (c)				
280	(c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.	(c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.	(c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI; or	(c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI; or Text Origin: Council Mandate
Article 24(1), point (ca)				
280a			(d) where available and applicable, a European cybersecurity certification scheme as specified in Article 18(9) and (10) at any assurance level.	<u>(d) where available and applicable, a European cybersecurity certification scheme as specified in Article 18(10).</u> Text Origin: Council Mandate
Article 24(1), point (ca)				
280b		<u>(ca) a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881 in accordance with Article 18(4).</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 24(2)			
281	2. Where, in assessing the compliance of the critical product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer or the manufacturer's authorised representative has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to either of the following procedures:	2. Where, in assessing the compliance of the critical product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer or the manufacturer's authorised representative has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes <u>at assurance level 'substantial' or "high"</u> as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to either of the following procedures:	2. Where, in assessing the compliance of the ~~critical~~ product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer ~~or the manufacturer's authorised representative~~ has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to ~~either~~ any of the following procedures:	2. Where, in assessing the compliance of the <u>(critical)</u> 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~~ <u>has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes (at required / assurance level 'substantial' or "high")</u> 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~~ <u>any</u> of the following procedures: 'critical' to be aligned with Article 6 Council and EP check of 'assurance level' Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 24(2), point (-a)				
281a			(c) where available and applicable, a European cybersecurity certification scheme as specified in Article 18(9) and (10) at the required assurance level. moved to line 283a	
Article 24(2), point (a)				
282	(a) EU-type examination procedure (based on module B) provided for in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or	(a) EU-type examination procedure (based on module B) provided for in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or	(a) ~~the~~ EU-type examination procedure (based on module B) ~~set out provided for~~ in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; ~~or~~	(a) <u>the</u> EU-type examination procedure (based on module B) ~~provided for~~ <u>set out</u> in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or Text Origin: Council Mandate
Article 24(2), point (b)				
283	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI-; or	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI. Text Origin: Council Mandate
Article 24(2), point (ba)				
283a			(c) where available and applicable, a European	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			cybersecurity certification scheme as specified in Article 18(9) and (10) at the required assurance level.	
	Article 24(2), point (ba)			
283b		<u>2a. Harmonised standards, common specifications or European cybersecurity certification schemes shall be in place for six months before the conformity assessment procedure referred to in paragraph 2 of this Article applies. In the six months prior to the application of paragraph 2 of this Article, or where, harmonised standards, common specifications or European cybersecurity certification schemes do not exist, manufacturers shall demonstrate the conformity of the critical product with digital elements of class I as set out in Annex III by means of the procedure referred to in paragraph 1 of this Article.</u>		EP to provide new wording / check
	Article 24(3)			
284	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	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	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	3. Where the product is a <u>(critical)</u> product with digital elements of class II as set out in Annex III, the manufacturer ~~or the manufacturer's authorised representative~~ <u>shall</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:	demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:	demonstrate conformity with the essential requirements set out in Annex I by using ~~one~~ any of the following procedures:	demonstrate conformity with the essential requirements set out in Annex I by using ~~one~~ any of the following procedures: (critical) to be aligned with Article 6 Text Origin: Council Mandate
	Article 24(3), point (-a)			
284a		<u>(-a) a European cybersecurity certificate, under a European cybersecurity certification scheme at assurance level 'substantial' or 'high' pursuant to Regulation (EU) 2019/881;</u>		See line 286a
	Article 24(3), point (a)			
285	(a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or	(a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or	(a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; ~~or~~	(a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; ~~or~~ Text Origin: Council Mandate
	Article 24(3), point (b)			
286	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI; or	(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI; ~~or~~ or

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Council Mandate
	Article 24(3), point (ba)			
y	286a		(c) where available and applicable, a European cybersecurity certification scheme as specified in Article 18 (9) and (10) at the required assurance level.	<u>(c) where available and applicable, a European cybersecurity certification scheme as specified in Article 18(10) (at the required assurance level / at assurance level 'substantial' or 'high' pursuant to Regulation (EU) 2019/881).</u> Council and Ep check 'assurance level' Text Origin: Council Mandate
	Article 24(3), point (bb)			
y	286b		3aa. Products listed in Annex IIIa shall demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:	To be aligned with Articles 6 and (Council) 6a
	Article 24(3), point (bc)			
y	286c		(a) a European cybersecurity certification scheme in accordance with Article 6a (1) , or,	To be aligned with Articles 6 and (Council) 6a
	Article 24(3), point (bd)			
y	286d		(b) where the conditions in Article 6a (1) are not met, any of the	To be aligned with Articles 6 and

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			procedures referred to in paragraph 3 of this Article.	(Council) 6a
Article 24(3), point (be)				
286e		<u>3a. The Commission shall request ENISA to prepare the missing candidate schemes in accordance with Article 48 of Regulation (EU) 2019/881.</u>		COM to provide text for recital 39.
Article 24(4)				
287	4. Manufacturers of products with digital elements that are classified as EHR systems under the scope of Regulation [the European Health Data Space Regulation] shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by Regulation [Chapter III of the European Health Data Space Regulation].	4. Manufacturers of products with digital elements that are classified as EHR systems under ~~the scope of~~ Regulation [the European Health Data Space Regulation] shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by Regulation [Chapter III of the European Health Data Space Regulation].	4. Manufacturers of products with digital elements that are classified as EHR systems under the scope of Regulation [the European Health Data Space Regulation] shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by Regulation [Chapter III of the European Health Data Space Regulation].	4. Manufacturers of products with digital elements that are classified as EHR systems under ~~the scope of~~ Regulation [the European Health Data Space Regulation] shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by Regulation [Chapter III of the European Health Data Space Regulation]. Text Origin: EP Mandate
Article 24(5)				
288	5. Notified bodies shall take into account the specific interests and needs of small and medium sized enterprises (SMEs) when setting the	5. Notified bodies shall take into account the specific interests and needs of ~~small and medium sized enterprises (SMEs)~~ <u>microenterprises</u>	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 <u>microenterprises and</u> small and ~~medium sized~~ <u>medium-sized</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs.	<u>and small and medium-sized enterprises</u> when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs. <u>The Commission shall ensure appropriate financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and on small and medium-sized enterprises.</u>	(SMEs) SMEs, including start-ups, shall be taken into account when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs.	enterprises, <u>including start-ups, shall be taken into account</u> ~~(SMEs)~~ when setting the fees for conformity assessment procedures and ~~reduce~~ those fees <u>shall be reduced</u> proportionately to their specific interests and needs. <u>(The Commission shall ensure appropriate financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and on small and medium-sized enterprises.)</u> Council and COM check / provide new wording. EP could consider moving text to Article 24a. Text Origin: EP Mandate
Article 24a				
288a			Article 24a Support measures for small and micro enterprises	EP check (medium-sized, and against other articles) and Council check on 'technical documentation'. COM to provide text on line 288g (technical documentation)

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 24a(1)			
Y	288b		1. Member States may undertake the following actions, tailored to the needs of small and micro enterprises:	Y
	Article 24a(1), point (a)			
Y	288c		(a) organise specific awareness raising and training activities about the application of this Regulation;	Y
	Article 24a(1), point (b)			
Y	288d		(b) where appropriate, establish a dedicated channel for communication with small and micro enterprises and, as appropriate, local public authorities to provide advice and respond to queries about the implementation of this Regulation.	Y
	Article 24a(1), point (c)			
Y	288e		(c) where appropriate, support testing and conformity assessment activities.	Y

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 24a(2)				
288f			2. The Commission shall ensure the development of guidance for small and micro enterprises in relation to the implementation of this Regulation.	
Article 24a(3)				
288g			3. Small and micro enterprises may provide the elements of the technical documentation specified in Annex V in a simplified manner. For this purpose, the Commission, in consultation with the market surveillance authorities, shall establish a simplified technical documentation form targeted at the needs of small and micro enterprises. Where a small or micro enterprise opts to provide the information required in Annex V in a simplified manner, it shall use the form referred to in this paragraph. Notified bodies shall accept the form for the purpose of conformity assessment.	
Article 24a				
288h		<u>Article 24a</u> <u>Mutual recognition agreements</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 24a, first paragraph			
288i		<u>1. In order to promote international trade, the Commission shall endeavour to conclude Mutual Recognition Agreements (MRAs) with third countries. The Union shall establish MRAs only with third countries that are on a comparable level of technical development and have a compatible approach concerning conformity assessment. The MRAs shall ensure the same level of protection as that provided for by this Regulation.</u>		<u>1. Taking into account the level of technical development and the approach on conformity assessment of a third country, the Union may conclude Mutual Recognition Agreements with such third countries, in order to promote and facilitate international trade.</u>
CHAPTER IV				
289	CHAPTER IV NOTIFICATION OF CONFORMITY ASSESSMENT BODIES	CHAPTER IV NOTIFICATION OF CONFORMITY ASSESSMENT BODIES	CHAPTER IV NOTIFICATION OF CONFORMITY ASSESSMENT BODIES	CHAPTER IV NOTIFICATION OF CONFORMITY ASSESSMENT BODIES Text Origin: Commission Proposal
Article 25				
290	Article 25 Notification	Article 25 Notification	Article 25 Notification	Article 25 Notification Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 25, first paragraph				
291	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 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. Text Origin: Council Mandate
Article 26				
292	Article 26 Notifying authorities	Article 26 Notifying authorities	Article 26 Notifying authorities	Article 26 Notifying authorities Text Origin: Commission Proposal
Article 26(1)				
293	1. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, including compliance with Article 31.	1. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, including compliance with Article 31.	1. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, including compliance with Article 31.	1. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, including compliance with Article 31. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 26(2)				
294	2. Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with Regulation (EC) No 765/2008.	2. Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with Regulation (EC) No 765/2008.	2. Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with Regulation (EC) No 765/2008.	2. Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with Regulation (EC) No 765/2008. Text Origin: Commission Proposal
Article 26(2a)				
294a			3. Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 to a body which is not a governmental entity, that body shall be a legal entity and shall comply mutatis mutandis with the requirements laid down in [Article 27] of this Regulation. In addition it shall have arrangements to cover liabilities arising out of its activities	<u>3. Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 to a body which is not a governmental entity, that body shall be a legal entity and shall comply mutatis mutandis with the requirements laid down in [Article 27] of this Regulation. In addition it shall have arrangements to cover liabilities arising out of its activities</u> Text Origin: Council Mandate
Article 26(2b)				
294b			4. The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3.	<u>4. The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3.</u>

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Council Mandate
Article 27				
295	Article 27 Requirements relating to notifying authorities	Article 27 Requirements relating to notifying authorities	Article 27 Requirements relating to notifying authorities	Article 27 Requirements relating to notifying authorities Text Origin: Commission Proposal
Article 27(1)				
296	1. A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs.	1. A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs.	1. A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs.	1. A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs. Text Origin: Commission Proposal
Article 27(2)				
297	2. A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities.	2. A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities.	2. A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities.	2. A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities. Text Origin: Commission Proposal
Article 27(3)				
298	3. A notifying authority shall be	3. A notifying authority shall be	3. A notifying authority shall be	3. A notifying authority shall be

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment.	organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment.	organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment.	organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment. Text Origin: Commission Proposal
Article 27(4)				
299	4. A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis.	4. A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis.	4. A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis.	4. A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis. Text Origin: Commission Proposal
Article 27(5)				
300	5. A notifying authority shall safeguard the confidentiality of the information it obtains.	5. A notifying authority shall safeguard the confidentiality of the information it obtains.	5. A notifying authority shall safeguard the confidentiality of the information it obtains.	5. A notifying authority shall safeguard the confidentiality of the information it obtains. Text Origin: Commission Proposal
Article 27(6)				
301	6. A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.	6. A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.	6. A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.	6. A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
	Article 27(6a)			
Y	301a	<u>6a. A notifying authority shall minimise administrative burden and fees imposed, in particular, on microenterprises and small and medium-sized enterprises.</u>		EP to check correct placement
	Article 28			
G	302	Article 28 Information obligation on notifying authorities	Article 28 Information obligation on notifying authorities	Article 28 Information obligation on notifying authorities Text Origin: Commission Proposal
	Article 28(1)			
G	303	1. Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes thereto.	1. Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes thereto.	1. Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes thereto. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 28(1a)				
y	303a	<u>1a. Member States shall, by ... [24 months after the date of entry into force of this Regulation], ensure that there is a sufficient number of notified bodies in the Union to carry out conformity assessments, in order to avoid bottlenecks and hindrances to market entry.</u>	PUBLIC	<u>1a. Member States shall strive to, by ... [24 months after the date of entry into force of this Regulation], ensure that there is a sufficient number of notified bodies in the Union to carry out conformity assessments, in order to avoid bottlenecks and hindrances to market entry.</u> Council will provide alternative text for operative part Text Origin: EP Mandate
Article 28(2)				
g	304	2. The Commission shall make that information publicly available.	2. The Commission shall make that information publicly available.	2. The Commission shall make that information publicly available. Text Origin: Commission Proposal
Article 29				
g	305	Article 29 Requirements relating to notified bodies	Article 29 Requirements relating to notified bodies	Article 29 Requirements relating to notified bodies Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 29(1)				
306	1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12.	1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12.	1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12.	1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12. Text Origin: Commission Proposal
Article 29(2)				
307	2. A conformity assessment body shall be established under national law and have legal personality.	2. A conformity assessment body shall be established under national law and have legal personality.	2. A conformity assessment body shall be established under national law and have legal personality.	2. A conformity assessment body shall be established under national law and have legal personality. Text Origin: Commission Proposal
Article 29(3), first subparagraph				
308	3. A conformity assessment body shall be a third-party body independent of the organisation or the product it assesses.	3. A conformity assessment body shall be a third-party body independent of the organisation or the product it assesses.	3. A conformity assessment body shall be a third-party body independent of the organisation or the product it assesses.	3. A conformity assessment body shall be a third-party body independent of the organisation or the product it assesses. Text Origin: Commission Proposal
Article 29(3), second subparagraph				
309	A body belonging to a business association or professional federation representing undertakings involved in the design, development,	A body belonging to a business association or professional federation representing undertakings involved in the design, development,	A body belonging to a business association or professional federation representing undertakings involved in the design, development,	A body belonging to a business association or professional federation representing undertakings involved in the design, development,

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	production, provision, assembly, use or maintenance of products with digital elements which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered such a body.	production, provision, assembly, use or maintenance of products with digital elements which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered such a body.	production, provision, assembly, use or maintenance of products with digital elements which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered such a body.	production, provision, assembly, use or maintenance of products with digital elements which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered such a body. Text Origin: Commission Proposal
Article 29(4), first subparagraph				
310	4. A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.	4. A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.	4. A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, importer, distributor , installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.	4. A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, <u>importer, distributor</u> , installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes. Text Origin: Council Mandate
Article 29(4), second subparagraph				
311	A conformity assessment body, its	A conformity assessment body, its	A conformity assessment body, its	A conformity assessment body, its

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, development, production, the marketing, installation, use or maintenance of those products, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services.	top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, development, production, the marketing, installation, use or maintenance of those products, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services.	top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, development, production, import, distribution , the marketing, installation, use or maintenance of those products, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services.	top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, development, production, <u>import, distribution</u> , the marketing, installation, use or maintenance of those products, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services. Text Origin: Council Mandate
Article 29(4), third subparagraph				
312	Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.	Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.	Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.	Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities. Text Origin: Commission Proposal
Article 29(5)				
313	5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities	5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities	5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities	5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.	with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.	with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.	with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities. Text Origin: Commission Proposal
Article 29(6), first subparagraph				
314	6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VI and in relation to which it has been notified, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.	6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VI and in relation to which it has been notified, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.	6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VI and in relation to which it has been notified, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.	6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VI and in relation to which it has been notified, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Text Origin: Commission Proposal
Article 29(6), second subparagraph				
315	At all times and for each conformity assessment procedure and each kind	At all times and for each conformity assessment procedure and each kind	At all times and for each conformity assessment procedure and each kind	At all times and for each conformity assessment procedure and each kind

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary:	or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary:	or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary:	or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary: Text Origin: Commission Proposal
Article 29(6), second subparagraph, point (a)				
316	(a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;	(a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;	(a) ~~staff~~ personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;	(a) ~~staff~~ personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks; Text Origin: Council Mandate
Article 29(6), second subparagraph, point (b)				
317	(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency and the ability of reproduction of those procedures. It shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities;	(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency and the ability of reproduction of those procedures. It shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities;	(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency and the ability of reproduction of those procedures. It shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities;	(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency and the ability of reproduction of those procedures. It shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 29(6), second subparagraph, point (c)				
318	(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process.	(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process.	(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process.	(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process. Text Origin: Commission Proposal
Article 29(6), third subparagraph				
319	It shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities.	It shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities.	It shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities.	It shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities. Text Origin: Commission Proposal
Article 29(7)				
320	7. The personnel responsible for carrying out conformity assessment activities shall have the following:	7. The personnel responsible for carrying out conformity assessment activities shall have the following:	7. The personnel responsible for carrying out conformity assessment activities shall have the following:	7. The personnel responsible for carrying out conformity assessment activities shall have the following: Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 29(7), point (a)				
321	(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;	(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;	(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;	(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified; Text Origin: Commission Proposal
Article 29(7), point (b)				
322	(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;	(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;	(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;	(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments; Text Origin: Commission Proposal
Article 29(7), point (c)				
323	(c) appropriate knowledge and understanding of the essential requirements, of the applicable harmonised standards and of the relevant provisions of Union harmonisation legislation and of its implementing acts;	(c) appropriate knowledge and understanding of the essential requirements <u>set out in Annex I</u> , of the applicable harmonised standards and of the relevant provisions of Union harmonisation legislation and of its implementing acts;	(c) appropriate knowledge and understanding of the essential requirements set out in Annex I , of the applicable harmonised standards as well as the common specifications and of the relevant provisions of Union harmonisation legislation and of its implementing acts;	(c) appropriate knowledge and understanding of the essential requirements <u>set out in Annex I</u> , of the applicable harmonised standards <u>as well as the common specifications</u> and of the relevant provisions of Union harmonisation legislation and of its implementing acts; Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 29(7), point (d)				
G	324	(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.	(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.	(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out. Text Origin: Commission Proposal
Article 29(7), point (da)				
Y	324a	<u>7a. Member States and the Commission shall put in place appropriate measures to ensure sufficient availability of skilled professionals, in order to minimise bottlenecks in the activities of conformity assessment bodies and facilitate the compliance of economic operators with this Regulation.</u>		To be discussed together with Article 6b Text Origin: EP Mandate
Article 29(8), first subparagraph				
G	325	8. The impartiality of the conformity assessment bodies, their top level management and of the assessment personnel shall be guaranteed.	8. The impartiality of the conformity assessment bodies, their top level management and of the assessment personnel shall be guaranteed.	8. The impartiality of the conformity assessment bodies, their top level management and of the assessment personnel shall be guaranteed. Text Origin: Commission Proposal
Article 29(8), second subparagraph				

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
326	The remuneration of the top level management and assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.	The remuneration of the top level management and assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.	The remuneration of the top level management and assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.	The remuneration of the top level management and assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments. Text Origin: Commission Proposal
Article 29(9)				
327	9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.	9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.	9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.	9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment. Text Origin: Commission Proposal
Article 29(10)				
328	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	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	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	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

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.	are carried out. Proprietary rights shall be protected <u>in accordance with Article 52</u> . The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.	are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.	are carried out. Proprietary rights shall be protected <u>in accordance with Article 52</u> . The conformity assessment body shall have documented procedures ensuring compliance with this paragraph. EP check (IMCO) Text Origin: EP Mandate
Article 29(11)				
329	11. Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 40 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group.	11. Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 40 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group.	11. Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 40 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group.	11. Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 40 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group. Text Origin: Commission Proposal
Article 29(12)				
330	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 <u>in accordance with Article 37(2)</u> , in particular taking into account the interests of	12. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, in particular taking into account the interests of SMEs in relation to fees.	12. Conformity assessment bodies shall operate in accordance with a set of consistent, fair, <u>proportionate</u> and reasonable terms and conditions, <u>while avoiding unnecessary burdens for economic operators</u> , in

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		~~SMEs~~ <u>microenterprises and small and medium-sized enterprises</u> in relation to fees.		particular taking into account the interests of ~~SMEs~~ <u>microenterprises and small and medium-sized enterprises</u> in relation to fees. Text Origin: EP Mandate
Article 30				
331	Article 30 Presumption of conformity of notified bodies	Article 30 Presumption of conformity of notified bodies	Article 30 Presumption of conformity of notified bodies	Article 30 Presumption of conformity of notified bodies Text Origin: Commission Proposal
Article 30, first paragraph				
332	Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union it shall be presumed to comply with the requirements set out in Article 29 in so far as the applicable harmonised standards cover those requirements.	Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union it shall be presumed to comply with the requirements set out in Article 29 in so far as the applicable harmonised standards cover those requirements.	Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union it shall be presumed to comply with the requirements set out in Article 29 in so far as the applicable harmonised standards cover those requirements.	Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union it shall be presumed to comply with the requirements set out in Article 29 in so far as the applicable harmonised standards cover those requirements. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 31				
333	Article 31 Subsidiaries of and subcontracting by notified bodies	Article 31 Subsidiaries of and subcontracting by notified bodies	Article 31 Subsidiaries of and subcontracting by notified bodies	Article 31 Subsidiaries of and subcontracting by notified bodies Text Origin: Commission Proposal
Article 31(1)				
334	1. Where a notified body subcontracts specific tasks connected with conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 29 and shall inform the notifying authority accordingly.	1. Where a notified body subcontracts specific tasks connected with conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 29 and shall inform the notifying authority accordingly.	1. Where a notified body subcontracts specific tasks connected with conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 29 and shall inform the notifying authority accordingly.	1. Where a notified body subcontracts specific tasks connected with conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 29 and shall inform the notifying authority accordingly. Text Origin: Commission Proposal
Article 31(2)				
335	2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established.	2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established.	2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established.	2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 31(3)				
336	3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the manufacturer.	3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the manufacturer.	3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the manufacturer.	3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the manufacturer. Text Origin: Commission Proposal
Article 31(4)				
337	4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.	4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.	4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.	4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation. Text Origin: Commission Proposal
Article 32				
338	Article 32 Application for notification	Article 32 Application for notification	Article 32 Application for notification	Article 32 Application for notification Text Origin: Commission Proposal
Article 32(1)				
339	1. A conformity assessment body shall submit an application for	1. A conformity assessment body shall submit an application for	1. A conformity assessment body shall submit an application for	1. A conformity assessment body shall submit an application for

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	notification to the notifying authority of the Member State in which it is established.	notification to the notifying authority of the Member State in which it is established.	notification to the notifying authority of the Member State in which it is established.	notification to the notifying authority of the Member State in which it is established. Text Origin: Commission Proposal
Article 32(2)				
340	2. That application shall be accompanied by a description of the conformity assessment activities, the conformity assessment procedure or procedures and the product or products for which that body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 29.	2. That application shall be accompanied by a description of the conformity assessment activities, the conformity assessment procedure or procedures and the product or products for which that body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 29.	2. That application shall be accompanied by a description of the conformity assessment activities, the conformity assessment procedure or procedures and the product or products for which that body claims to be competent, as well as by an accreditation certificate, where ~~one exists~~ applicable , issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 29.	2. That application shall be accompanied by a description of the conformity assessment activities, the conformity assessment procedure or procedures and the product or products for which that body claims to be competent, as well as by an accreditation certificate, where ~~one exists~~ applicable , issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 29. Text Origin: Council Mandate
Article 32(3)				
341	3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article	3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article	3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article	3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	29.	29.	29.	29. Text Origin: Commission Proposal
Article 33				
342	Article 33 Notification procedure	Article 33 Notification procedure	Article 33 Notification procedure	Article 33 Notification procedure Text Origin: Commission Proposal
Article 33(1)				
343	1. Notifying authorities may notify only conformity assessment bodies, which have satisfied the requirements laid down in Article 29.	1. Notifying authorities may notify only conformity assessment bodies, which have satisfied the requirements laid down in Article 29.	1. Notifying authorities may notify only conformity assessment bodies, which have satisfied the requirements laid down in Article 29.	1. Notifying authorities may notify only conformity assessment bodies, which have satisfied the requirements laid down in Article 29. Text Origin: Commission Proposal
Article 33(2)				
344	2. The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations (NANDO) information system developed and managed by the Commission.	2. The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations (NANDO) information system developed and managed by the Commission.	2. The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations (NANDO) information system developed and managed by the Commission.	2. The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations (NANDO) information system developed and managed by the Commission. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 33(3)			
345	3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and product or products concerned and the relevant attestation of competence.	3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and product or products concerned and the relevant attestation of competence.	3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and product or products concerned and the relevant attestation of competence.	3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and product or products concerned and the relevant attestation of competence. Text Origin: Commission Proposal
	Article 33(4)			
346	4. Where a notification is not based on an accreditation certificate as referred to in Article 32(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 29.	4. Where a notification is not based on an accreditation certificate as referred to in Article 32(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 29.	4. Where a notification is not based on an accreditation certificate as referred to in Article 32(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 29.	4. Where a notification is not based on an accreditation certificate as referred to in Article 32(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 29. Text Origin: Commission Proposal
	Article 33(5), first subparagraph			
347	5. The body concerned may perform	5. The body concerned may perform	5. The body concerned may perform	5. The body concerned may perform

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification where an accreditation certificate is used or within two months of a notification where accreditation is not used.	the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification where an accreditation certificate is used or within two months of a notification where accreditation is not used.	the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification where an accreditation certificate is used or within two months of a notification where accreditation is not used.	the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification where an accreditation certificate is used or within two months of a notification where accreditation is not used. Text Origin: Commission Proposal
Article 33(5), second subparagraph				
348	Only such a body shall be considered a notified body for the purposes of this Regulation.	Only such a body shall be considered a notified body for the purposes of this Regulation.	Only such a body shall be considered a notified body for the purposes of this Regulation.	Only such a body shall be considered a notified body for the purposes of this Regulation. Text Origin: Commission Proposal
Article 33(6)				
349	6. The Commission and the other Member States shall be notified of any subsequent relevant changes to the notification.	6. The Commission and the other Member States shall be notified of any subsequent relevant changes to the notification.	6. The Commission and the other Member States shall be notified of any subsequent relevant changes to the notification.	6. The Commission and the other Member States shall be notified of any subsequent relevant changes to the notification. Text Origin: Commission Proposal
Article 34				
350	Article 34 Identification numbers and lists of notified bodies	Article 34 Identification numbers and lists of notified bodies	Article 34 Identification numbers and lists of notified bodies	Article 34 Identification numbers and lists of notified bodies

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 34(1), first subparagraph				
351	1. The Commission shall assign an identification number to a notified body.	1. The Commission shall assign an identification number to a notified body.	1. The Commission shall assign an identification number to a notified body.	1. The Commission shall assign an identification number to a notified body. Text Origin: Commission Proposal
Article 34(1), second subparagraph				
352	It shall assign a single such number even where the body is notified under several Union acts.	It shall assign a single such number even where the body is notified under several Union acts.	It shall assign a single such number even where the body is notified under several Union acts.	It shall assign a single such number even where the body is notified under several Union acts. Text Origin: Commission Proposal
Article 34(2), first subparagraph				
353	2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been allocated to them and the activities for which they have been notified.	2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been allocated to them and the activities for which they have been notified.	2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been allocated to them and the activities for which they have been notified.	2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been allocated to them and the activities for which they have been notified. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 34(2), second subparagraph				
354	The Commission shall ensure that that list is kept up to date.	The Commission shall ensure that that list is kept up to date.	The Commission shall ensure that that list is kept up to date.	The Commission shall ensure that that list is kept up to date. Text Origin: Commission Proposal
Article 35				
355	Article 35 Changes to notifications	Article 35 Changes to notifications	Article 35 Changes to notifications	Article 35 Changes to notifications Text Origin: Commission Proposal
Article 35(1)				
356	1. Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 29, or that it is failing to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.	1. Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 29, or that it is failing to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.	1. Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 29, or that it is failing to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.	1. Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 29, or that it is failing to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 35(2)				
357	2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying Member State shall take appropriate steps to ensure that the files of that body are either processed by another notified body or kept available for the responsible notifying and market surveillance authorities at their request.	2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying Member State shall take appropriate steps to ensure that the files of that body are either processed by another notified body or kept available for the responsible notifying and market surveillance authorities at their request.	2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying Member State shall take appropriate steps to ensure that the files of that body are either processed by another notified body or kept available for the responsible notifying and market surveillance authorities at their request.	2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying Member State shall take appropriate steps to ensure that the files of that body are either processed by another notified body or kept available for the responsible notifying and market surveillance authorities at their request. Text Origin: Commission Proposal
Article 36				
358	Article 36 Challenge of the competence of notified bodies	Article 36 Challenge of the competence of notified bodies	Article 36 Challenge of the competence of notified bodies	Article 36 Challenge of the competence of notified bodies Text Origin: Commission Proposal
Article 36(1)				
359	1. The Commission shall investigate all cases where it doubts, or doubt is brought to its attention regarding the competence of a notified body or the continued fulfilment by a notified body of the requirements and responsibilities to which it is subject.	1. The Commission shall investigate all cases where it doubts, or doubt is brought to its attention regarding the competence of a notified body or the continued fulfilment by a notified body of the requirements and responsibilities to which it is subject.	1. The Commission shall investigate all cases where it doubts, or doubt is brought to its attention regarding the competence of a notified body or the continued fulfilment by a notified body of the requirements and responsibilities to which it is subject.	1. The Commission shall investigate all cases where it doubts, or doubt is brought to its attention regarding the competence of a notified body or the continued fulfilment by a notified body of the requirements and responsibilities to which it is subject.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 36(2)				
360	2. The notifying Member State shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the body concerned.	2. The notifying Member State shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the body concerned.	2. The notifying Member State shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the body concerned.	2. The notifying Member State shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the body concerned. Text Origin: Commission Proposal
Article 36(3)				
361	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 sensitive information obtained in the course of its investigations is treated confidentially.	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 sensitive information obtained in the course of its investigations is treated confidentially. Text Origin: Commission Proposal
Article 36(4)				
362	4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including de-notification if necessary.	4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including de-notification if necessary.	4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including de-notification if necessary.	4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including de-notification if necessary.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 37				
363	Article 37 Operational obligations of notified bodies	Article 37 Operational obligations of notified bodies	Article 37 Operational obligations of notified bodies	Article 37 Operational obligations of notified bodies Text Origin: Commission Proposal
Article 37(1)				
364	1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 24 and Annex VI.	1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 24 and Annex VI.	1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 24 and Annex VI.	1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 24 and Annex VI. Text Origin: Commission Proposal
Article 37(2)				
365	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	2. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for economic operators. <u>with consideration for microenterprises and small and medium-sized enterprises.</u> Conformity assessment bodies shall perform their activities taking due account of the size of an	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	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, <u>with consideration for microenterprises and small and medium-sized enterprises,</u> the sector

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	technology in question and the mass or serial nature of the production process.	undertaking, the sector in which it operates, its structure, the degree of complexity <u>and the risk exposure</u> of the product <u>type and</u> technology in question and the mass or serial nature of the production process.	technology in question and the mass or serial nature of the production process.	in which it operates, its structure, the degree of complexity <u>and the cybersecurity risk level</u> of the product <u>and</u> technology in question and the mass or serial nature of the production process. Text Origin: EP Mandate
Article 37(3)				
366	3. Notified bodies shall however respect the degree of rigour and the level of protection required for the compliance of the product with the provisions of Regulation.	3. Notified bodies shall however respect the degree of rigour and the level of protection required for the compliance of the product with the provisions of Regulation.	3. Notified bodies shall however respect the degree of rigour and the level of protection required for the compliance of the product with the provisions of Regulation.	3. Notified bodies shall however respect the degree of rigour and the level of protection required for the compliance of the product with the provisions of Regulation. Text Origin: Commission Proposal
Article 37(4)				
367	4. Where a notified body finds that requirements laid down in Annex I or in corresponding harmonised standards or in common specifications as referred to in Article 19 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a conformity certificate.	4. Where a notified body finds that requirements laid down in Annex I or in corresponding harmonised standards or in common specifications as referred to in Article 19 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a conformity certificate.	4. Where a notified body finds that requirements laid down in Annex I or in corresponding harmonised standards or in common specifications as referred to in Article 19 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a ~~conformity~~ certificate of conformity .	4. Where a notified body finds that requirements laid down in Annex I or in corresponding harmonised standards or in common specifications as referred to in Article ~~19~~ 18 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a ~~conformity~~ certificate <u>of conformity</u> . Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 37(5)				
368	5. Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product no longer complies with the requirements laid down in this Regulation, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the certificate if necessary.	5. Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product no longer complies with the requirements laid down in this Regulation, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the certificate if necessary.	5. Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product no longer complies with the requirements laid down in this Regulation, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the certificate if necessary.	5. Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product no longer complies with the requirements laid down in this Regulation, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the certificate if necessary. Text Origin: Commission Proposal
Article 37(6)				
369	6. Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any certificates, as appropriate.	6. Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any certificates, as appropriate.	6. Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any certificates, as appropriate.	6. Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any certificates, as appropriate. Text Origin: Commission Proposal
Article 37a				
369a			Article 37a Appeal against decisions of notified bodies	<u>Article 37a</u> <u>Appeal against decisions of notified bodies</u> Text Origin: Council Mandate

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 37a(1)			
369b			1. Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.	<u>1. Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.</u> Text Origin: Council Mandate
	Article 38			
370	Article 38 Information obligation on notified bodies	Article 38 Information obligation on notified bodies	Article 38 Information obligation on notified bodies	Article 38 Information obligation on notified bodies Text Origin: Commission Proposal
	Article 38(1)			
371	1. Notified bodies shall inform the notifying authority of the following:	1. Notified bodies shall inform the notifying authority of the following:	1. Notified bodies shall inform the notifying authority of the following:	1. Notified bodies shall inform the notifying authority of the following: Text Origin: Commission Proposal
	Article 38(1), point (a)			
372	(a) any refusal, restriction, suspension or withdrawal of a certificate;	(a) any refusal, restriction, suspension or withdrawal of a certificate;	(a) any refusal, restriction, suspension or withdrawal of a certificate;	(a) any refusal, restriction, suspension or withdrawal of a certificate; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 38(1), point (b)				
373	(b) any circumstances affecting the scope of and conditions for notification;	(b) any circumstances affecting the scope of and conditions for notification;	(b) any circumstances affecting the scope of and conditions for notification;	(b) any circumstances affecting the scope of and conditions for notification; Text Origin: Commission Proposal
Article 38(1), point (c)				
374	(c) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;	(c) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;	(c) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;	(c) any request for information which they have received from market surveillance authorities regarding conformity assessment activities; Text Origin: Commission Proposal
Article 38(1), point (d)				
375	(d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.	(d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.	(d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.	(d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting. Text Origin: Commission Proposal
Article 38(2)				
376	2. Notified bodies shall provide the	2. Notified bodies shall provide the	2. Notified bodies shall provide the	2. Notified bodies shall provide the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same products with relevant information on issues relating to negative and, on request, positive conformity assessment results.	other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same products with relevant information on issues relating to negative and, on request, positive conformity assessment results.	other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same products with relevant information on issues relating to negative and, on request, positive conformity assessment results.	other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same products with relevant information on issues relating to negative and, on request, positive conformity assessment results. Text Origin: Commission Proposal
Article 39				
377	Article 39 Exchange of experience	Article 39 Exchange of experience	Article 39 Exchange of experience	Article 39 Exchange of experience Text Origin: Commission Proposal
Article 39, first paragraph				
378	The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification policy.	The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification policy.	The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification policy.	The Commission shall provide for the organisation of exchange of experience between the Member States' national authorities responsible for notification policy. Text Origin: Commission Proposal
Article 40				
379	Article 40 Coordination of notified bodies	Article 40 Coordination of notified bodies	Article 40 Coordination of notified bodies	Article 40 Coordination of notified bodies

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 40(1)				
380	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, <u>taking also in account the need to reduce the administrative burden and fees</u> , 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 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 and properly operated in the form of a cross-sectoral group of notified bodies. Text Origin: Commission Proposal
Article 40(2)				
381	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.	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. Text Origin: Commission Proposal
CHAPTER V				
382	CHAPTER V MARKET SURVEILLANCE AND ENFORCEMENT	CHAPTER V MARKET SURVEILLANCE AND ENFORCEMENT	CHAPTER V MARKET SURVEILLANCE AND ENFORCEMENT	CHAPTER V MARKET SURVEILLANCE AND ENFORCEMENT Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 41				
383	Article 41 Market surveillance and control of products with digital elements in the Union market	Article 41 Market surveillance and control of products with digital elements in the Union market	Article 41 Market surveillance and control of products with digital elements in the Union market	Article 41 Market surveillance and control of products with digital elements in the Union market Text Origin: Commission Proposal
Article 41(1)				
384	1. Regulation (EU) 2019/1020 shall apply to the products with digital elements within the scope of this Regulation.	1. Regulation (EU) 2019/1020 shall apply to the products with digital elements <u>that fall</u> within the scope of this Regulation.	1. Regulation (EU) 2019/1020 shall apply to the products with digital elements within the scope of this Regulation.	
Article 41(2)				
385	2. Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation.	2. Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation.	2. Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation.	2. Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation. Text Origin: Commission Proposal
Article 41(3)				
386	3. Where relevant, the market	3. Where relevant, the market	3. Where relevant, the market	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	surveillance authorities shall cooperate with the national cybersecurity certification authorities designated under Article 58 of Regulation (EU) 2019/881 <del> and exchange information on a regular basis.</del> <i>With respect to the supervision of the implementation of the reporting obligations, competent authorities and CSIRTs designated pursuant to ~~Article 11 of this Regulation, the designated market surveillance authorities shall cooperate with ENISA~~ Directive (EU) 2022/2555 and exchange information on a regular basis.</i>	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 the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 and ENISA.	
Article 41(3a)				
386a		<u>3a. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 11 of this Regulation, the designated market surveillance authorities shall cooperate with ENISA. The market surveillance authorities may request ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 43, market surveillance authorities may request ENISA to provide non-binding evaluations of compliance of products with digital elements.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 41(4)				
387	4. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, and exchange information on a regular basis.	4. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, and exchange information on a regular basis.	4. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, and exchange information on a regular basis.	4. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, and exchange information on a regular basis. Text Origin: Commission Proposal
Article 41(5), first subparagraph				
388	5. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing these authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 8 of this Article if such guidance and advice concerns the processing of personal data.	5. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing these authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 8 of this Article if such guidance and advice concerns the processing of personal data.	5. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing these authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 8 of this Article if such guidance and advice concerns the processing of personal data.	5. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing these authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 8 of this Article if such guidance and advice concerns the processing of personal data. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 41(5), second subparagraph				
389	Authorities supervising Union data protection law shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks. They shall inform the designated market surveillance authorities of the Member State concerned of any such request.	Authorities supervising Union data protection law shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks. They shall inform the designated market surveillance authorities of the Member State concerned of any such request.	Authorities supervising Union data protection law shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks. They shall inform the designated market surveillance authorities of the Member State concerned of any such request.	Authorities supervising Union data protection law shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks. They shall inform the designated market surveillance authorities of the Member State concerned of any such request. Text Origin: Commission Proposal
Article 41(6)				
390	6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and human resources to fulfil their tasks under this Regulation.	6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and human resources, <u>with appropriate cybersecurity skills, in order</u> to fulfil their tasks under this Regulation.	6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial, human and technical and human resources, including, where appropriate, processing automation tools , to fulfil their tasks under this Regulation.	
Article 41(7)				
391	7. The Commission shall facilitate the exchange of experience between designated market surveillance authorities.	7. The Commission shall facilitate the <u>regular and structured</u> exchange of experience between designated market surveillance authorities.	7. The Commission shall facilitate the exchange of experience between designated market surveillance authorities.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 41(8)				
392	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 <u>as well as on non-technical risk factors</u> , with the support of <u>CSIRTs, ENISA and</u> 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.	
Article 41(8a)				
392a		<u>8a. Market surveillance authorities shall be equipped to receive complaints by consumers in accordance with Article 11 of Regulation 2019/1020, including by establishing clear and accessible mechanisms to facilitate reporting of vulnerabilities, incidents and cyber threats.</u>		
Article 41(9)				
393	9. The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition	9. The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition	9. The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law.	authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law. <u>Market surveillance authorities shall provide the Commission with data about the average support period set by the manufacturers, as well as when available the average expected product lifetime, and disaggregated per category of product with digital elements. The Commission shall analyse this information and publish it in a publicly accessible and user-friendly database.</u>	authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law.	
Article 41(9a)				
393a		<u>9a. The Commission shall evaluate the reported data including pursuant to paragraph 9 of this Article for the purpose of the reports referred to in Article 56. Where the reported data suggests an increased level of non-compliance in specific categories of products, the Commission, after consulting the Expert Group and ADCO, may recommend that surveillance authorities focus closely on the product categories concerned.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 41(10)				
394	10. For products with digital elements in the scope of this Regulation classified as high-risk AI systems according to Article [Article 6] of the Regulation [the AI Regulation], the market surveillance authorities designated for the purposes of the Regulation [the AI Regulation] shall be the authorities responsible for market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall cooperate, as appropriate, with the market surveillance authorities designated pursuant to this Regulation and, with respect to the supervision of the implementation of the reporting obligations pursuant to Article 11, with ENISA. Market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall in particular inform market surveillance authorities designated pursuant to this Regulation of any finding relevant for the fulfilment of their tasks in relation to the implementation of this Regulation.	10. For products with digital elements ~~##that fall within~~ the scope of this Regulation classified as high-risk AI systems according to Article [Article 6] of the Regulation [the AI Regulation], the market surveillance authorities designated for the purposes of the Regulation [the AI Regulation] shall be the authorities responsible for market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall cooperate, as appropriate, with the market surveillance authorities designated pursuant to this Regulation and, with respect to the supervision of the implementation of the reporting obligations pursuant to Article 11, with ENISA. Market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall in particular inform market surveillance authorities designated pursuant to this Regulation of any finding relevant for the fulfilment of their tasks in relation to the implementation of this Regulation.	10. For products with digital elements in the scope of this Regulation classified as high-risk AI systems according to Article [Article 6] of the Regulation [the AI Regulation], the market surveillance authorities designated for the purposes of the Regulation [the AI Regulation] shall be the authorities responsible for market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall cooperate, as appropriate, with the market surveillance authorities designated pursuant to this Regulation and, with respect to the supervision of the implementation of the reporting obligations pursuant to Article 11, with the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 and ENISA. Market surveillance authorities designated pursuant to Regulation [the AI Regulation] shall in particular inform market surveillance authorities designated pursuant to this Regulation of any finding relevant for the fulfilment of their tasks in relation to the implementation of this Regulation.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 41(11)				
395	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).~~ <u>An ADCO for cyber resilience of products with digital elements</u> 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. <u>In particular, this ADCO shall exchange best practices and, where relevant, cooperate with the Expert Group and ENISA as well as the Cooperation Group and the CSIRTs Network referred to under Directive (EU) 2022/2555.</u>	11. A dedicated administrative cooperation group (ADCO) shall be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. This ADCO shall be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of single liaison offices.	
Article 41(11a)				
395a			11a. ADCO may publish relevant statistics on categories of products with digital elements, including about the average expected product lifetime, as specified by the manufacturer pursuant to Article 10 (10a), per category of products with digital elements.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 41(11a)				
395b		<u>11a. Market surveillance authorities shall facilitate the involvement of stakeholders, including scientific, research and consumer organisations, in their activities.</u>		
Article 42				
396	Article 42 Access to data and documentation	Article 42 Access to data and documentation	Article 42 Access to data and documentation	Article 42 Access to data and documentation Text Origin: Commission Proposal
Article 42, first paragraph				
397	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 necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data, in a language easily understood by them , required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the respective economic operator.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 43				
398	Article 43 Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk	Article 43 Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk	Article 43 Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk	Article 43 Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk Text Origin: Commission Proposal
Article 43(1), first subparagraph				
399	1. Where the market surveillance authority of a Member State has sufficient reasons to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall carry out an evaluation of the product with digital elements concerned in respect of its compliance with all the requirements laid down in this Regulation. The relevant economic operators shall cooperate as necessary with the market surveillance authority.	1. Where the market surveillance authority of a Member State has sufficient reasons to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall carry out <u>without undue delay, and where appropriate in cooperation with CSIRT</u> , an evaluation of the product with digital elements concerned in respect of its compliance with all the requirements laid down in this Regulation. The relevant economic operators shall cooperate as necessary with the market surveillance authority.	1. Where the market surveillance authority of a Member State has sufficient reasons to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall carry out an evaluation of the product with digital elements concerned in respect of its compliance with all the requirements laid down in this Regulation. The relevant economic operators shall cooperate as necessary with the market surveillance authority.	
Article 43(1), second subparagraph				
400	Where, in the course of that evaluation, the market surveillance authority finds that the product with	Where, in the course of that evaluation, the market surveillance authority finds that the product with	Where, in the course of that evaluation, the market surveillance authority finds that the product with	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant <i>economic</i> 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.	digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant economic operator to take ~~all~~ appropriate corrective actions to bring the product with digital elements into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as ~~it~~ the market surveillance authority may prescribe.	
Article 43(1), third subparagraph				
401	The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the appropriate corrective actions.	The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the appropriate corrective actions.	The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the ~~appropriate~~ corrective actions.	
Article 43(1a)				
401a		<i><u>1a. Where the market surveillance authority of a Member State has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk or threats to national security in light of non-technical risk factors, it shall issue targeted recommendations to economic operators aimed at ensuring that</u></i>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>appropriate corrective actions are put in place.</u>		
Article 43(2)				
402	2. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the operator to take.	2. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the operator to take.	2. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the economic operator to take.	
Article 43(3)				
403	3. The manufacturer shall ensure that all appropriate corrective action is taken in respect of all the products with digital elements concerned that it has made available on the market throughout the Union.	3. The manufacturer shall ensure that all appropriate corrective action is taken in respect of all the products with digital elements concerned that it has made available on the market throughout the Union.	3. The ~~manufacturer~~ economic operator shall ensure that ~~all~~ any appropriate corrective action is taken in respect of all the products with digital elements concerned that it has made available on the market throughout the Union.	
Article 43(4), first subparagraph				
404	4. 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	4. 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	4. Where the ~~manufacturer of a product with digital elements~~ economic operator does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph, the market surveillance authority	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	measures to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it.	measures to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it.	shall take ~~all~~ appropriate provisional measures to prohibit or restrict that product with digital elements from being made available on its national market, to withdraw it from that market or to recall it.	
Article 43(4), second subparagraph				
405	That authority shall inform the Commission and the other Member States, without delay, of those measures.	That authority shall inform the Commission and the other Member States, without delay, of those measures.	That authority shall ~~inform~~ notify the Commission and the other Member States, without delay, of those measures.	
Article 43(5)				
406	5. The information referred to in paragraph 4 shall include all available details, in particular the data necessary for the identification of the non-compliant products with digital elements, the origin of the product with digital elements, the nature of the alleged non-compliance and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authority shall indicate whether the non-compliance is due to one or more of the following:	5. The information referred to in paragraph 4 shall include all available details, in particular the data necessary for the identification of the non-compliant products with digital elements, the origin of the product with digital elements, the nature of the alleged non-compliance and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authority shall indicate whether the non-compliance is due to one or more of the following:	5. The information referred to in paragraph 4 shall include all available details, in particular the data necessary for the identification of the non-compliant ~~products~~ product with digital elements, the origin of ~~the~~ that product with digital elements, the nature of the alleged non-compliance and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant economic operator. In particular, the market surveillance authority shall indicate whether the non-compliance is due to one or more of the following:	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 43(5), point (a)				
407	(a) a failure of the product or of the processes put in place by the manufacturer to meet the essential requirements set out in Annex I;	(a) a failure of the product or of the processes put in place by the manufacturer to meet the essential requirements set out in Annex I;	(a) a failure of the product with digital elements or of the processes put in place by the manufacturer to meet the essential requirements set out in Annex I;	
Article 43(5), point (b)				
408	(b) shortcomings in the harmonised standards, cybersecurity certification schemes, or common specifications, referred to in Article 18.	(b) shortcomings in the harmonised standards, cybersecurity certification schemes, or common specifications, referred to in Article 18.	(b) shortcomings in the harmonised standards, cybersecurity certification schemes, or common specifications, referred to in Article 18.	(b) shortcomings in the harmonised standards, cybersecurity certification schemes, or common specifications, referred to in Article 18. Text Origin: Commission Proposal
Article 43(6)				
409	6. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product concerned, and, in the event of disagreement with the notified national measure, of their objections.	6. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product concerned, and, in the event of disagreement with the notified national measure, of their objections.	6. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product with digital elements concerned, and, in the event of disagreement with the notified national measure, of their objections.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 43(7)				
410	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. 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~~ notification referred to in paragraph 4, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the economic operator concerned in accordance with Article 18 of Regulation (EU) 2019/1020.	
Article 43(8)				
411	8. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product concerned, such as withdrawal of the product from their market, without delay.	8. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product concerned, such as withdrawal of the product from their market, without delay.	8. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product with digital elements concerned, such as withdrawal of ~~the that~~ product from their market, without delay.	
Article 44				
412	Article 44 Union safeguard procedure	Article 44 Union safeguard procedure	Article 44 Union safeguard procedure	Article 44 Union safeguard procedure Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Article 44(1)				
413	1. Where, within three months of receipt of the notification referred to in Article 43(4), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union legislation, the Commission shall without delay enter into consultation with the relevant Member State and the economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within nine months from the notification referred to in Article 43(4) and notify such decision to the Member State concerned.	1. Where, within three months of receipt of the notification referred to in Article 43(4), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union legislation, the Commission shall without delay enter into consultation with the relevant Member State and the economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within nine months from the notification referred to in Article 43(4) and notify such decision to the Member State concerned.	1. Where, within three months of receipt of the notification referred to in Article 43(4), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union ~~legislation~~ law, the Commission shall without delay enter into consultation with the relevant Member State and the economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within nine months from the notification referred to in Article 43(4) and notify ~~such~~ that decision to the Member State concerned.	
Article 44(2)				
414	2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant product with digital elements is withdrawn from their market, and shall inform the	2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant product with digital elements is withdrawn from their market, and shall inform the	2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant product with digital elements is withdrawn from their market, and shall inform the	2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant product with digital elements is withdrawn from their market, and shall inform the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure.	Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure.	Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure.	Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure. Text Origin: Commission Proposal
Article 44(3)				
415	3. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in the harmonised standards, the Commission shall apply the procedure provided for in Article 10 of Regulation (EU) No 1025/2012.	3. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in the harmonised standards, the Commission shall apply the procedure provided for in Article 10 of Regulation (EU) No 1025/2012.	3. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in the harmonised standards, the Commission shall apply the procedure provided for in Article 10 of Regulation (EU) No 1025/2012.	
Article 44(4)				
416	4. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in a European cybersecurity certification scheme as referred to in Article 18, the Commission shall consider whether to amend or repeal the implementing act as referred to in Article 18(4) that specifies the presumption of conformity concerning that	4. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in a European cybersecurity certification scheme as referred to in Article 18, the Commission shall consider whether to amend or repeal the implementing act as referred to in Article 18(4) that specifies the presumption of conformity concerning that	4. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in a European cybersecurity certification scheme as referred to in Article 18, the Commission shall consider whether to amend or repeal the implementing act as referred to in Article 18(4) that specifies the presumption of conformity concerning that	4. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in a European cybersecurity certification scheme as referred to in Article 18, the Commission shall consider whether to amend or repeal the implementing act as referred to in Article 18(4) that specifies the presumption of conformity concerning that

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	certification scheme.	certification scheme.	certification scheme.	certification scheme. Text Origin: Commission Proposal
Article 44(5)				
417	5. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in common specifications as referred to in Article 19, the Commission shall consider whether to amend or repeal the implementing act referred to in Article 19 setting out those common specifications.	5. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in common specifications as referred to in Article 19, the Commission shall consider whether to amend or repeal the implementing act referred to in Article 19 setting out those common specifications.	5. Where the national measure is considered justified and the non-compliance of the product with digital elements is attributed to shortcomings in common specifications as referred to in Article ~~19~~ 18 , the Commission shall consider whether to amend or repeal the implementing act referred to in Article ~~19~~ 18 setting out those common specifications.	
Article 45				
418	Article 45 Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk	Article 45 Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk	Article 45 Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk	Article 45 Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk Text Origin: Commission Proposal
Article 45(1)				
419	1. Where the Commission has sufficient reasons to consider, including based on information	1. Where the Commission has sufficient ~~reasons~~ reason to consider, including based on information	1. Where the Commission has sufficient reasons to consider, including based on information	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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~~ shall request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.	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~~ shall inform the relevant market surveillance authorities. Where the market surveillance authorities to carry out an evaluation of that product with digital elements that may present a significant cybersecurity risk in respect of its compliance and follow with the requirements laid down in this Regulation, the procedures referred to in Article 43 Articles 43 and 44 shall apply.	
Article 45(1a)				
419a		<u><i>1a. Where the Commission has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of non-technical risk factors, it shall inform the relevant market surveillance authorities and issue targeted recommendations to economic operators aimed at ensuring that appropriate corrective actions are put in place.</i></u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 45(2)				
420	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 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~~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.	2. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product with digital elements referred to in paragraph 1 remains 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~~provide an analysis to support an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.	
Article 45(3)				
421	3. Based on ENISA's evaluation, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.	3. Based on ENISA's evaluation, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.	3. Based on ~~ENISA's~~the evaluation referred to in paragraph 2, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 45(4)				
422	4. On the basis of the consultation referred to in paragraph 3, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	4. On the basis of the consultation referred to in paragraph 3, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	4. On the basis of the consultation referred to in paragraph 3, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal of the product with digital elements from the market, or recalling of it , within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	
Article 45(5)				
423	5. The Commission shall immediately communicate the decision referred to in paragraph 4 to the relevant economic operator or operators. Member States shall implement the acts referred to in paragraph 4 without delay and shall inform the Commission accordingly.	5. The Commission shall immediately communicate the decision referred to in paragraph 4 to the relevant economic operator or operators. Member States shall implement the acts referred to in paragraph 4 without delay and shall inform the Commission accordingly.	5. The Commission shall immediately communicate the implementing acts ~~decision~~ referred to in paragraph 4 to the relevant economic operator or operators. Member States shall implement ~~the acts referred to in paragraph 4~~ those acts without delay and shall inform the Commission accordingly.	
Article 45(6)				
424	6. Paragraphs 2 to 5 are applicable for the duration of the exceptional situation that justified the	6. Paragraphs 2 to 5 are applicable for the duration of the exceptional situation that justified the	6. Paragraphs 2 to 5 are applicable for the duration of the exceptional situation that justified the	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Commission's intervention and for as long as the respective product is not brought in compliance with this Regulation.	Commission's intervention and for as long as the respective product is not brought in compliance with this Regulation.	Commission's intervention and for as long as the ~~respective product~~ product with digital elements concerned is not brought in compliance with this Regulation.	
Article 46				
425	Article 46 Compliant products with digital elements which present a significant cybersecurity risk	Article 46 Compliant products with digital elements which present a significant cybersecurity risk	Article 46 Compliant products with digital elements which present a significant cybersecurity risk	Article 46 Compliant products with digital elements which present a significant cybersecurity risk Text Origin: Commission Proposal
Article 46(1)				
426	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	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	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	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	system by essential entities of the type referred to in ~~Annex I to Article 3 of~~ Directive ~~XXX/XXXX (NIS2 EU)~~ <u>2022/2555</u> or to other aspects of public interest protection, it shall require the relevant <u>economic</u> 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.	~~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~~ it shall require an economic operator to take appropriate measures where, having performed an evaluation under Article 43, it finds that although a product with digital elements and the processes put in place by the manufacturer 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, are in compliance with this Regulation, it presents a significant cybersecurity risk as well as a risk to:	
Article 46(-1), first subparagraph, point (a)				
426a			(a) the health or safety of persons;	
Article 46(-1), first subparagraph, point (b)				
426b			(b) the compliance with obligations under Union or national law intended to protect	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			fundamental rights;	
Article 46(-1), first subparagraph, point (c)				
426c			(c) the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by entities of a type referred to in Annex I to Directive (EU) 2022/2555; or	
Article 46(-1), first subparagraph, point (d)				
426d			(d) other aspects of public interest protection.	
Article 46(-1), second subparagraph				
426e			The measures referred to in the first subparagraph may include measures to ensure that the product with digital elements concerned and the processes put in place by the manufacturer no longer present the relevant risks [when made available on the market], withdrawal from the market of the product with digital elements concerned, or recalling of it, and shall be commensurate with the nature of those risks.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 46(2)				
427	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 <i>economic</i> 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.	2. The manufacturer or other relevant <i>economic</i> 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. Text Origin: Council Mandate
Article 46(3)				
428	3. The Member State shall immediately inform the Commission and the other Member States about the measures taken pursuant to paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the products with digital elements concerned, the origin and the supply chain of those products with digital elements, the nature of the risk involved and the nature and duration of the national measures taken.	3. The Member State shall immediately inform the Commission and the other Member States about the measures taken pursuant to paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the products with digital elements concerned, the origin and the supply chain of those products with digital elements, the nature of the risk involved and the nature and duration of the national measures taken.	3. The Member State shall immediately inform the Commission and the other Member States about the measures taken pursuant to paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the products with digital elements concerned, the origin and the supply chain of those products with digital elements, the nature of the risk involved and the nature and duration of the national measures taken.	3. The Member State shall immediately inform the Commission and the other Member States about the measures taken pursuant to paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the products with digital elements concerned, the origin and the supply chain of those products with digital elements, the nature of the risk involved and the nature and duration of the national measures taken. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 46(4)				
429	4. The Commission shall without delay enter into consultation with the Member States and the relevant economic operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.	4. The Commission shall without delay enter into consultation with the Member States and the relevant economic operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.	4. The Commission shall without delay enter into consultation with the Member States and the relevant economic operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.	4. The Commission shall without delay enter into consultation with the Member States and the relevant economic operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures. Text Origin: Commission Proposal
Article 46(5)				
430	5. The Commission shall address its decision to the Member States.	5. The Commission shall address its decision to the Member States.	5. The Commission shall address its decision to the Member States.	5. The Commission shall address its decision to the Member States. Text Origin: Commission Proposal
Article 46(6)				
431	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	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	6. Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements, although compliant with this Regulation, presents the risks referred to in paragraph 1, it ~~may request~~ shall inform the relevant market	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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.	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.	
Article 46(7)				
432	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 ~~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 exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product with digital elements referred to in paragraph 6 continues to present the risks referred to in paragraph 1, and no effective measures have been taken by the relevant national market surveillance authorities, the Commission may request ENISA to ~~carry out~~ provide an analysis to support an evaluation of the risks presented by that product with digital elements and shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.	
Article 46(8)				
433	8. Based on ENISA's evaluation	8. Based on ENISA's evaluation	8. Based on ~~ENISA's~~ the evaluation	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	referred to in paragraph 7, the Commission may establish that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant operator or operators.	referred to in paragraph 7, the Commission ~~may~~ <u>shall</u> establish ~~that~~ a corrective or restrictive measure ~~is necessary~~ <u>if necessary</u> at Union level. To this end, it shall without delay consult the Member States concerned and the relevant operator or operators.	referred to in paragraph 7, the Commission may establish that a corrective or restrictive measure is necessary at Union level. To this end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.	
Article 46(9)				
434	9. On the basis of the consultation referred to in paragraph 8, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	9. On the basis of the consultation referred to in paragraph 8, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	9. On the basis of the consultation referred to in paragraph 8, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including ordering withdrawal of the product with digital elements from the market, or recalling of it , within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).	
Article 46(10)				
435	10. The Commission shall immediately communicate the decision referred to in the paragraph 9 to the relevant operator or operators. Member States shall implement such acts without delay	10. The Commission shall immediately communicate the decision referred to in the paragraph 9 to the relevant operator or operators. Member States shall implement such acts without delay	10. The Commission shall immediately communicate the ~~decision~~ implementing acts referred to in ~~the~~ paragraph 9 to the relevant economic operator or operators. Member States shall implement	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	and shall inform the Commission accordingly.	and shall inform the Commission accordingly.	~~such~~ those acts without delay and shall inform the Commission accordingly.	
Article 46(11)				
436	11. Paragraphs 6 to 10 shall apply for the duration of the exceptional situation that justified the Commission's intervention and for as long as the respective product continues to present the risks referred to in paragraph 1.	11. Paragraphs 6 to 10 shall apply for the duration of the exceptional situation that justified the Commission's intervention and for as long as the respective product continues to present the risks referred to in paragraph 1.	11. Paragraphs 6 to 10 shall apply for the duration of the exceptional situation that justified the Commission's intervention and for as long as the ~~respective product~~ product with digital elements concerned continues to present the risks referred to in paragraph 1.	
Article 47				
437	Article 47 Formal non-compliance	Article 47 Formal non-compliance	Article 47 Formal non-compliance	Article 47 Formal non-compliance Text Origin: Commission Proposal
Article 47(1)				
438	1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant manufacturer to end to the non-compliance concerned:	1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant manufacturer to end to the non-compliance concerned:	1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant manufacturer to end to the non-compliance concerned:	1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant manufacturer to end to the non-compliance concerned: Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 47(1), point (a)			
439	(a) the conformity marking has been affixed in violation of Articles 21 and 22;	(a) the conformity marking has been affixed in violation of Articles 21 and 22;	(a) the conformity marking has been affixed in violation of Articles 21 and 22;	
	Article 47(1), point (b)			
440	(b) the conformity marking has not been affixed;	(b) the conformity marking has not been affixed;	(b) the conformity marking has not been affixed;	
	Article 47(1), point (c)			
441	(c) the EU declaration of conformity has not been drawn up;	(c) the EU declaration of conformity has not been drawn up;	(c) the EU declaration of conformity has not been drawn up;	(c) the EU declaration of conformity has not been drawn up; Text Origin: Commission Proposal
	Article 47(1), point (d)			
442	(d) the EU declaration of conformity has not been drawn up correctly;	(d) the EU declaration of conformity has not been drawn up correctly;	(d) the EU declaration of conformity has not been drawn up correctly;	(d) the EU declaration of conformity has not been drawn up correctly; Text Origin: Commission Proposal
	Article 47(1), point (e)			
443	(e) the identification number of the notified body, which is involved in	(e) the identification number of the notified body, which is involved in	(e) the identification number of the notified body, which is involved in	(e) the identification number of the notified body, which is involved in

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	the conformity assessment procedure, where applicable, has not been affixed;	the conformity assessment procedure, where applicable, has not been affixed;	the conformity assessment procedure, where applicable, has not been affixed;	the conformity assessment procedure, where applicable, has not been affixed; Text Origin: Commission Proposal
Article 47(1), point (f)				
444	(f) the technical documentation is either not available or not complete.	(f) the technical documentation is either not available or not complete.	(f) the technical documentation is either not available or not complete.	(f) the technical documentation is either not available or not complete. Text Origin: Commission Proposal
Article 47(2)				
445	2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product with digital elements from being made available on the market or ensure that it is recalled or withdrawn from the market.	2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product with digital elements from being made available on the market or ensure that it is recalled or withdrawn from the market.	2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product with digital elements from being made available on the market or ensure that it is recalled or withdrawn from the market.	2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product with digital elements from being made available on the market or ensure that it is recalled or withdrawn from the market. Text Origin: Commission Proposal
Article 48				
446	Article 48 Joint activities of market surveillance authorities	Article 48 Joint activities of market surveillance authorities	Article 48 Joint activities of market surveillance authorities	Article 48 Joint activities of market surveillance authorities

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 48(1)				
447	1. Market surveillance authorities may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks.	1. Market surveillance authorities ~~may agree with other relevant authorities to~~ shall carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks.	1. Market surveillance authorities may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed on the market or made available on the market, in particular products with digital elements that are often found to present cybersecurity risks.	
Article 48(2)				
448	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 ~~may~~ 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~~ that fall within the scope of this Regulation with the requirements laid down by the latter.	2. The Commission or ENISA may propose joint activities for checking compliance with this Regulation ~~to be conducted by market surveillance authorities~~ based on indications or information of potential non-compliance across several Member States of products with digital elements falling in the scope of this Regulation with the requirements laid down ~~by the latter~~ herein .	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 48(3)				
449	3. The market surveillance authorities and the Commission, where applicable, shall ensure that the agreement to carry out joint activities does not lead to unfair competition between economic operators and does not negatively affect the objectivity, independence and impartiality of the parties to the agreement.	3. The market surveillance authorities and the Commission, where applicable, shall ensure that the agreement to carry out joint activities does not lead to unfair competition between economic operators and does not negatively affect the objectivity, independence and impartiality of the parties to the agreement.	3. The market surveillance authorities and the Commission, where applicable, the Commission , shall ensure that the agreement to carry out joint activities does not lead to unfair competition between economic operators and does not negatively affect the objectivity, independence and impartiality of the parties to the agreement.	
Article 48(4)				
450	4. A market surveillance authority may use any information resulting from the activities carried out as part of any investigation that it undertakes.	4. A market surveillance authority may use any information resulting from the activities carried out as part of any investigation that it undertakes.	4. A market surveillance authority may use any information resulting from the joint activities carried out as part of any investigation that it undertakes.	
Article 48(5)				
451	5. The market surveillance authority concerned and the Commission, where applicable, shall make the agreement on joint activities, including the names of the parties involved, available to the public.	5. The market surveillance authority concerned and the Commission, where applicable, shall make the agreement on joint activities, including the names of the parties involved, available to the public.	5. The market surveillance authority concerned and, where applicable, the Commission ~~the Commission, where applicable~~ , shall make the agreement on joint activities, including the names of the parties involved, available to the public.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 49				
452	Article 49 Sweeps	Article 49 Sweeps	Article 49 Sweeps	Article 49 Sweeps Text Origin: Commission Proposal
Article 49(1)				
453	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 ~~may decide to~~ <u>shall regularly</u> 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. <u>They shall include inspections of products acquired under a cover identity and shall aim to verify the compliance of those products with this Regulation.</u>	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.	
Article 49(2)				
454	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 ~~may, where appropriate,~~ <u>shall</u> 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 may, where appropriate, make the aggregated results publicly available.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 49(3)				
455	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 ~~may~~ 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 ~~may~~ 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.	3. ENISA may identify, in the performance of its tasks, including based on the notifications received according to Article 11(1) and (2), categories of products with digital elements for which sweeps may be organised. The proposal for sweeps shall be submitted to the ~~potential~~ coordinator referred to in paragraph 2 for the consideration of the market surveillance authorities.	
Article 49(4)				
456	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 may use the investigation powers set out in Articles 41 to 47 and any other powers conferred upon them by national law.	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.	
Article 49(5)				
457	5. Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.	5. Market surveillance authorities ~~may~~ shall invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.	5. Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
CHAPTER VI				
458	CHAPTER VI DELEGATED POWERS AND COMMITTEE PROCEDURE	CHAPTER VI DELEGATED POWERS AND COMMITTEE PROCEDURE	CHAPTER VI DELEGATED POWERS AND COMMITTEE PROCEDURE	CHAPTER VI DELEGATED POWERS AND COMMITTEE PROCEDURE Text Origin: Commission Proposal
Article 50				
459	Article 50 Exercise of the delegation	Article 50 Exercise of the delegation	Article 50 Exercise of the delegation	Article 50 Exercise of the delegation Text Origin: Commission Proposal
Article 50(1)				
460	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. Text Origin: Commission Proposal
Article 50(2)				
461	2. The power to adopt delegated acts referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) shall be conferred on the Commission.	2. The power to adopt delegated acts referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article <u>10(15), Article 11(5), Article 18(4), Article 19(1), Article</u> 20(5) and Article 23(5) shall be	2. The power to adopt delegated acts referred to in ~~Article 2(4), Article 6(2),- Article 6(3)~~ 6a(1), Article 6a(2) , Article 20(5) and Article 23(5) shall be conferred on the Commission for a period of five	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		conferred on the Commission.	years from ... [date of entry into force of this Regulation]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.	
Article 50(3)				
462	3. The delegation of power referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 10(15) , Article 11(5) , Article 18(4) , Article 19(1) , Article 20(5) and Article 23(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in ~~Article 2(4)~~ , Article 6(2), Article ~~6(3)~~ 6a(1) , Article ~~6(5)~~ 6a(2) , Article 20(5) and Article 23(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union ~~Official Journal of the European Union~~ or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 50(4)				
463	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the ~~Inter-institutional~~ Interinstitutional Agreement of 13 April 2016 on Better Law-Making.	
Article 50(5)				
464	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. Text Origin: Commission Proposal
Article 50(6)				
465	6. A delegated act adopted pursuant to Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article 20(5) and Article 23(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament	6. A delegated act adopted pursuant to Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article <u>10(15), Article 11(5), Article 18(4), Article 19(1), Article 20(5) or 20(5) and</u> Article 23(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the	6. A delegated act adopted pursuant to ~~Article 2(4),~~ Article 6(2), Article ~~6(3)~~ 6a(1) , Article ~~6(5)~~ 6a(2) , Article 20(5) and Article 23(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	
Article 51				
466	Article 51 Committee procedure	Article 51 Committee procedure	Article 51 Committee procedure	Article 51 Committee procedure Text Origin: Commission Proposal
Article 51(1)				
467	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. Text Origin: Commission Proposal
Article 51(2)				
468	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Article 51(3)			
469	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests. Text Origin: Commission Proposal
	CHAPTER VII			
470	CHAPTER VII CONFIDENTIALITY AND PENALTIES	CHAPTER VII CONFIDENTIALITY AND PENALTIES	CHAPTER VII CONFIDENTIALITY AND PENALTIES	CHAPTER VII CONFIDENTIALITY AND PENALTIES Text Origin: Commission Proposal
	Article 52			
471	Article 52 Confidentiality	Article 52 Confidentiality	Article 52 Confidentiality	Article 52 Confidentiality Text Origin: Commission Proposal
	Article 52(1)			
472	1. All parties involved in the	1. All parties involved in the	1. All parties involved in the	1. All parties involved in the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:	application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:	application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:	application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular: Text Origin: Commission Proposal
Article 52(1), point (a)				
473	(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 Council¹; 1. 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).	(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 Council¹; 1. 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).	(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 Council¹; 1. 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).	(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 Council¹; 1. 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). Text Origin: Commission Proposal
Article 52(1), point (b)				
474	(b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;	(b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;	(b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;	(b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 52(1), point (c)				
475	(c) public and national security interests;	(c) public and national security interests;	(c) public and national security interests;	(c) public and national security interests; Text Origin: Commission Proposal
Article 52(1), point (d)				
476	(d) integrity of criminal or administrative proceedings.	(d) integrity of criminal or administrative proceedings.	(d) integrity of criminal or administrative proceedings.	(d) integrity of criminal or administrative proceedings. Text Origin: Commission Proposal
Article 52(2)				
477	2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the market surveillance authorities and between market surveillance authorities and the Commission shall not be disclosed without the prior agreement of the originating market surveillance authority.	2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the market surveillance authorities and between market surveillance authorities and the Commission shall not be disclosed without the prior agreement of the originating market surveillance authority.	2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the market surveillance authorities and between market surveillance authorities and the Commission shall not be disclosed without the prior agreement of the originating market surveillance authority.	2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the market surveillance authorities and between market surveillance authorities and the Commission shall not be disclosed without the prior agreement of the originating market surveillance authority. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 52(3)				
478	3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law of the Member States.	3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law of the Member States.	3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law of the Member States.	3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law of the Member States. Text Origin: Commission Proposal
Article 52(4)				
479	4. The Commission and Member States may exchange, where necessary, sensitive information with relevant authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of protection.	4. The Commission and Member States may exchange, where necessary, sensitive information with relevant authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of protection.	4. The Commission and Member States may exchange, where necessary, sensitive information with relevant authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of protection.	4. The Commission and Member States may exchange, where necessary, sensitive information with relevant authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of protection. Text Origin: Commission Proposal
Article 53				
480	Article 53 Penalties	Article 53 Penalties	Article 53 Penalties	Article 53 Penalties Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Article 53(1)				
481	1. Member States shall lay down the rules on penalties applicable to infringements by economic operators of this Regulation and shall take all measures necessary to ensure that they are enforced. The penalties provided for shall be effective, proportionate and dissuasive.	1. Member States shall lay down the rules on penalties applicable to infringements by economic operators of this Regulation and shall take all measures necessary to ensure that they are enforced. The penalties provided for shall be effective, proportionate and dissuasive. <u>Member States shall ensure that those rules take into account the financial capabilities of microenterprises and small and medium-sized enterprises.</u>	1. Member States shall lay down the rules on penalties applicable to infringements by economic operators of this Regulation and shall take all measures necessary to ensure that they are ~~enforced~~ implemented . The penalties provided for shall be effective, proportionate and dissuasive.	
Article 53(2)				
482	2. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.	2. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them. <u>The Commission shall ensure that those rules and measures are applied in a uniform and consistent manner across the Union.</u>	2. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.	
Article 53(3)				
483	3. The non-compliance with the essential cybersecurity requirements	3. The non-compliance with the essential cybersecurity requirements	3. The non-compliance with the essential cybersecurity requirements	3. The non-compliance with the essential cybersecurity requirements

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	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.	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.	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.	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. Text Origin: Commission Proposal
Article 53(4)				
484	4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10 000 000 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.	4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10 000 000 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.	4. The non-compliance with ~~any other obligations~~ the obligations set out in Articles [Articles 12; 13; 14; 15; 16; 17; 20; 22 (1)-(4); 23 (1)-(4); 24(1)-(3); 29; 31; 37; 38; 42] under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.	
Article 53(5)				
485	5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000	5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000	5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000	5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.	000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.	000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.	000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher. Text Origin: Commission Proposal
Article 53(6)				
486	6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:	6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:	6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:	6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following: Text Origin: Commission Proposal
Article 53(6), point (a)				
487	(a) the nature, gravity and duration of the infringement and of its consequences;	(a) the nature, gravity and duration of the infringement and of its consequences;	(a) the nature, gravity and duration of the infringement and of its consequences;	(a) the nature, gravity and duration of the infringement and of its consequences; Text Origin: Commission Proposal
Article 53(6), point (aa)				
487a		<u>(aa) whether the infringement is unintentional;</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 53(6), point (b)				
488	(b) whether administrative fines have been already applied by other market surveillance authorities to the same operator for a similar infringement;	(b) whether administrative fines have been already applied by <u>the same or</u> other market surveillance authorities to the same operator for a similar infringement;	(b) whether administrative fines have been already applied by other market surveillance authorities to the same economic operator for a similar infringement;	
Article 53(6), point (c)				
489	(c) the size and market share of the operator committing the infringement.	(c) the size, <u>in particular with regard to microenterprises, small and medium sized-enterprises, including start-ups,</u> and market share of the operator committing the infringement.	(c) the size and market share of the economic operator committing the infringement.	
Article 53(7)				
490	7. Market surveillance authorities that apply administrative fines shall share this information with the market surveillance authorities of other Member States through the information and communication system referred to in Article 34 of Regulation (EU) 2019/1020.	7. Market surveillance authorities that apply administrative fines shall share this information with the market surveillance authorities of other Member States through the information and communication system referred to in Article 34 of Regulation (EU) 2019/1020.	7. Market surveillance authorities that apply administrative fines shall ~~share this information with~~ communicate this to the market surveillance authorities of other Member States through the information and communication system referred to in Article 34 of Regulation (EU) 2019/1020.	
Article 53(8)				
491	8. Each Member State shall lay down rules on whether and to what extent administrative fines may be	8. Each Member State shall lay down rules on whether and to what extent administrative fines may be	8. Each Member State shall lay down rules on whether and to what extent administrative fines may be	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	imposed on public authorities and bodies established in that Member State.	imposed on public authorities and bodies established in that Member State.	imposed on public authorities and public bodies established in that Member State.	
Article 53(9)				
492	9. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or other bodies according to the competences established at national level in those Member States. The application of such rules in those Member States shall have an equivalent effect.	9. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or other bodies according to the competences established at national level in those Member States. The application of such rules in those Member States shall have an equivalent effect.	9. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or other bodies according to the competences established at national level in those Member States. The application of such rules in those Member States shall have an equivalent effect.	9. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or other bodies according to the competences established at national level in those Member States. The application of such rules in those Member States shall have an equivalent effect. Text Origin: Commission Proposal
Article 53(10)				
493	10. Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement.	10. Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement.	10. Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement.	10. Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 53a				
493a		<u>Article 53a</u> <u>Allocation of the revenue from penalties</u>		
Article 53a, first paragraph				
493b		<u>1. Member States shall allocate the revenues from the penalties referred to in Article 53(1) to projects raising the level of cybersecurity within the Union. Those projects shall aim at least to one of the following:</u>		
Article 53a, first paragraph, point (a)				
493c		<u>(a) increase the number of skilled professionals in the field of cybersecurity, notably women;</u>		
Article 53a(1), point (b)				
493d		<u>(b) increase capacity-building for microenterprises and small and medium-sized enterprises in order to facilitate their compliance with this Regulation;</u>		
Article 53a(1), point (c)				
493e		<u>(c) improve public awareness of</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>cyber threats, with particular regard to their prevention and management;</u>		
Article 53a(1), point (d)				
493f		<u>(d) develop tools to increase the resilience of Union undertakings to cyber-enabled intellectual property theft.</u>		
CHAPTER VIII				
494	CHAPTER VIII TRANSITIONAL AND FINAL PROVISIONS	CHAPTER VIII TRANSITIONAL AND FINAL PROVISIONS	CHAPTER VIII TRANSITIONAL AND FINAL PROVISIONS	CHAPTER VIII TRANSITIONAL AND FINAL PROVISIONS Text Origin: Commission Proposal
Article 54				
495	Article 54 Amendment to Regulation (EU) 2019/1020	Article 54 Amendment to Regulation (EU) 2019/1020	Article 54 Amendment to Regulation (EU) 2019/1020	Article 54 Amendment to Regulation (EU) 2019/1020 Text Origin: Commission Proposal
Article 54, first paragraph				
496	In Annex I to Regulation (EU) 2019/1020 the following point is added:	In Annex I to Regulation (EU) 2019/1020 the following point is added:	In Annex I to Regulation (EU) 2019/1020 the following point is added:	In Annex I to Regulation (EU) 2019/1020 the following point is added:

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Article 54, first paragraph, amending provision, numbered paragraph (71)				
497	, 71. [Regulation XXX][Cyber Resilience Act].	, 71. <u>71.</u> [Regulation XXX] [Cyber Resilience Act].	, 71. [Regulation XXX][Cyber Resilience Act].	
Article 54a				
497a			Article 54a Representative actions	
Article 54, first paragraph, amending provision, Article(1)				
497b			1. Directive (EU) 2020/1828 shall apply to the representative actions brought against infringements by economic operators of provisions of this Regulation that harm, or may harm, the collective interests of consumers.	
Article 54b				
497c			Article 54b Amendment to Directive (EU) 2020/1828	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 54, first paragraph, amending provision, Article(1), first subparagraph				
497d			1. In Annex I to Directive (EU) 2020/1828, the following point is added:	
Article 54, first paragraph, amending provision, Article(1), second subparagraph				
497e			'(XX) [Regulation XXX][Cyber Resilience Act]'	
Article 54a				
497f		<u>Article 54a</u> <u>Amendment to Directive (EU) 2020/1828</u>		
Article 54a(1), first paragraph				
497g		<u>1. In Annex I to Directive (EU) 2020/1828 of the European Parliament and of the Council' the following point is added:</u> <u>1. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 54a(1), first paragraph, second subparagraph				
497h		<u>'67. [Regulation XXX] [Cyber Resilience Act]'</u>		
Article 55				
498	Article 55 Transitional provisions	Article 55 Transitional provisions	Article 55 Transitional provisions	Article 55 Transitional provisions Text Origin: Commission Proposal
Article 55(1)				
499	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 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 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 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. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 55(2)				
500	2. Products with digital elements that have been placed on the market before [date of application of this Regulation referred to in Article 57], shall be subject to requirements of this Regulation only if, from that date, those products are subject to substantial modifications in their design or intended purpose.	2. Products with digital elements that have been placed on the market before [date of application of this Regulation referred to in Article 57], shall be subject to requirements of this Regulation only if, from that date, those products are subject to substantial modifications in their design or intended purpose.	2. Products with digital elements that have been placed on the market before [date of application of this Regulation referred to in Article 57], shall be subject to requirements of this Regulation only if, from that date, those products are subject to substantial modifications in their design or intended purpose.	2. Products with digital elements that have been placed on the market before [date of application of this Regulation referred to in Article 57], shall be subject to requirements of this Regulation only if, from that date, those products are subject to substantial modifications in their design or intended purpose. Text Origin: Commission Proposal
Article 55(3)				
501	3. By way of derogation from paragraph 2, the obligations laid down in Article 11 shall apply to all products with digital elements within the scope of this Regulation that have been placed on the market before [date of application of this Regulation referred to in Article 57].	3. By way of derogation from paragraph 2, the obligations laid down in Article 11 shall apply to all products with digital elements <u>that fall</u> within the scope of this Regulation that have been placed on the market before [date of application of this Regulation referred to in Article 57].	3. By way of derogation from paragraph 2, the obligations laid down in Article 11 shall apply to all products with digital elements within the scope of this Regulation that have been placed on the market before [date of application of this Regulation referred to in Article 57].	3. By way of derogation from paragraph 2, the obligations laid down in Article 11 shall apply to all products with digital elements within the scope of this Regulation that have been placed on the market before [date of application of this Regulation referred to in Article 57]. Text Origin: Commission Proposal
Article 55(3a)				
501a		<u>3a. Until the date of application of this Regulation, manufacturers may comply with the requirements of this Regulation on a voluntary basis. Where manufacturers comply</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>with this Regulation with regard to their products with digital elements, they shall be considered also to comply with Delegated Regulation (EU) 2022/30.</u> <u>The Commission shall repeal Delegated Regulation (EU) 2022/30 on the same date of application of this Regulation.</u>		
Article 56				
502	Article 56 Evaluation and review	Article 56 Evaluation and review	Article 56 Evaluation and review	Article 56 Evaluation and review Text Origin: Commission Proposal
Article 56, first paragraph				
503	By [36 months after the date of application of this Regulation] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.	<u>1.</u> By [36 months after the date of application of this Regulation] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.	By [36 months after the date of application of this Regulation] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.	
Article 56, second paragraph				
503a		<u>2. Every year when presenting the Draft Budget for the following year.</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<i><u>the Commission shall submit a detailed assessment of ENISA's tasks under this Regulation as set out in Annex VIa and other relevant Union law and shall detail the financial and human resources needed to fulfil those tasks.</u></i>		
Article 57				
504	Article 57 Entry into force and application	Article 57 Entry into force and application	Article 57 Entry into force and application	Article 57 Entry into force and application Text Origin: Commission Proposal
Article 57, first paragraph				
505	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. Text Origin: Commission Proposal
Article 57, second paragraph				
506	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 [~~24~~ 36 months after the date of entry into force of this Regulation]. However Article 11 shall apply from [~~12~~ 18 months after the date of entry into force of this Regulation].	It shall apply from [24 36 months after the date of entry into force of this Regulation]. However Article 11 shall apply from [~~12~~ 24 months after the date of entry into force of this Regulation].	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Article 57, third paragraph				
507	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States. Text Origin: Commission Proposal
Formula				
508	Done at Brussels,	Done at ~~Brussels~~ ...	Done at Brussels,	
Formula				
509	For the European Parliament	For the European Parliament	For the European Parliament	For the European Parliament Text Origin: Commission Proposal
Formula				
510	The President	The President	The President	The President Text Origin: Commission Proposal
Formula				
511	For the Council	For the Council	For the Council	For the Council Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Formula				
512	The President	The President	The President	The President Text Origin: Commission Proposal
Annex I				
513	Annex I	Annex I	Annex I	Annex I Text Origin: Commission Proposal
Annex I, first paragraph				
514	ESSENTIAL CYBERSECURITY REQUIREMENTS	ESSENTIAL CYBERSECURITY REQUIREMENTS	ESSENTIAL CYBERSECURITY REQUIREMENTS	ESSENTIAL CYBERSECURITY REQUIREMENTS Text Origin: Commission Proposal
Annex I, Part I				
515	Part I 1. Security requirements relating to the properties of products with digital elements	Part I 1. Security requirements relating to the properties of products with digital elements	Part I 1. ~~Security requirements relating to the properties of products with digital elements~~ SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, second paragraph				
516	(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	(1) Products with digital elements shall be designed, developed and produced in such a way that they ~~ensure~~ enable an appropriate level of cybersecurity based on the risks;	
Annex I, third paragraph				
517	(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;	<i>deleted</i>	<i>deleted</i>	
Annex I, fourth paragraph				
518	(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:	(3) On the basis of the <u>cybersecurity</u> risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:	(3) On the basis of the cybersecurity risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:	(3) On the basis of the <u>cybersecurity</u> risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall: <u>Text Origin: Council Mandate</u>
Annex I, fourth paragraph, point (aa)				
518a			(aa) be placed on the market without any known exploitable vulnerabilities;	
Annex I, fourth paragraph, point (-a)				
518b		<u>(-a) be made available without known exploitable vulnerabilities;</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, fourth paragraph, point (a)				
519	(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	(a) be ~~delivered~~ <u>made available</u> with a secure by default configuration, <u>unless otherwise agreed between the parties in a business-to-business context,</u> including the possibility to reset the product to its original state <u>while retaining all installed security updates;</u>	(a) be ~~delivered~~ placed on the market with a secure by default configuration, including the possibility to reset the product to its original state, and including a default setting that security updates be installed automatically according to requirements in point (aaa) of this section and Annex II (9), with a clear and easy- to-use opt-out mechanism.	
Annex I, fourth paragraph, point (aaa)				
519a			(aaa) where applicable under Annex I,1 (3)a of this section, set as a default setting – which can be switched off – that security updates are installed automatically on products with digital elements if not installed within a certain timeframe;	
Annex I, fourth paragraph, point (aa)				
519b		<u>(aa) where technically feasible, be made available on the market with functional separation of security updates from functionality update;</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, fourth paragraph, point (ab)				
519c		<u>(ab) ensure automatic security updates with a clear and easy-to-use opt-out mechanism and the notification of available updates to users;</u>		
Annex I, fourth paragraph, point (b)				
520	(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems; Text Origin: Commission Proposal
Annex I, fourth paragraph, point (c)				
521	(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 encrypting relevant data at rest or in transit by state of the art mechanisms, <u>and by using other technical means;</u>	(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;	
Annex I, fourth paragraph, point (d)				
522	(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands,	(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands,	(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;	programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions <u>or possible unauthorised access</u> ;	programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;	
Annex I, fourth paragraph, point (e)				
523	(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');	(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');	(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended ~~use~~ purpose of the product ('minimisation of data');	
Annex I, fourth paragraph, point (f)				
524	(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	(f) protect the availability of essential <u>and basic</u> functions, <u>also after an incident</u> , including <u>with backup management</u> , and the resilience ~~against~~ and mitigation ~~of measures against~~ denial of service attacks;	(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	
Annex I, fourth paragraph, point (g)				
525	(g) minimise their own negative impact on the availability of services provided by other devices or networks;	(g) minimise their own negative impact on the availability of services provided by other devices or networks;	(g) minimise ~~their own~~ the negative impact by themselves or connected devices on the availability of services provided by other devices or networks;	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, fourth paragraph, point (h)				
526	(h) be designed, developed and produced to limit attack surfaces, including external interfaces;	(h) be designed, developed and produced to limit attack surfaces, including external interfaces;	(h) be designed, developed and produced to limit attack surfaces, including external interfaces;	(h) be designed, developed and produced to limit attack surfaces, including external interfaces; Text Origin: Commission Proposal
Annex I, fourth paragraph, point (i)				
527	(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 an incident using appropriate exploitation mitigation mechanisms and techniques;	(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 an incident using appropriate exploitation mitigation mechanisms and techniques; Text Origin: Commission Proposal
Annex I, fourth paragraph, point (j)				
528	(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 recording and/or monitoring <u>capabilities for</u> relevant internal activity, including the access to or modification of data, services or functions, <u>with an opt-out mechanism for the user</u> ;	(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;	
Annex I, fourth paragraph, point (k)				
529	(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through	<i>deleted</i>	(k) ~~ensure~~ enable that vulnerabilities can be addressed through security updates, including, where applicable,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	automatic updates and the notification of available updates to users.		through automatic updates by default, but with a clear and easy-to-use opt-out mechanism, and where applicable through ~~and the~~ notification of available updates to users, and the option to temporarily postpone them;	
Annex I, fourth paragraph, point (l)				
529a			(l) provide the possibility for users to securely and easily remove all data and settings and, where such data can be transferred to other products or systems, ensure this is done in a secure manner.	
Annex I, fourth paragraph, point (ka)				
529b		<u>(ka) enable users to securely withdraw and remove their data on a permanent basis.</u>		
Annex I, Part II				
530	Part II 2. Vulnerability handling requirements	Part II 2. Vulnerability handling requirements	Part II 2. Vulnerability handling requirements	Part II 2. Vulnerability handling requirements Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, fifth paragraph				
531	Manufacturers of the products with digital elements shall:	Manufacturers of the products with digital elements shall:	Manufacturers of the products with digital elements shall:	Manufacturers of the products with digital elements shall: Text Origin: Commission Proposal
Annex I, sixth paragraph				
532	(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;	(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;	(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;	(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product; Text Origin: Commission Proposal
Annex I, seventh paragraph				
533	(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 vulnerabilities without delay, including by providing security updates <u>installed automatically where applicable in accordance with Section I</u> ;	(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, eighth paragraph				
534	(3) apply effective and regular tests and reviews of the security of the product with digital elements;	(3) apply effective and regular tests and reviews of the security of the product with digital elements;	(3) apply effective and regular tests and reviews of the security of the product with digital elements;	(3) apply effective and regular tests and reviews of the security of the product with digital elements; Text Origin: Commission Proposal
Annex I, ninth paragraph				
535	(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~~ <u>share and publicly</u> disclose information about fixed vulnerabilities <u>in a controlled way</u> , 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 <u>clear and accessible</u> 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 user friendly information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, tenth paragraph				
536	(5) put in place and enforce a policy on coordinated vulnerability disclosure;	(5) put in place and enforce a policy on coordinated vulnerability disclosure;	(5) put in place and enforce a policy on coordinated vulnerability disclosure;	(5) put in place and enforce a policy on coordinated vulnerability disclosure; Text Origin: Commission Proposal
Annex I, eleventh paragraph				
537	(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements; Text Origin: Commission Proposal
Annex I, twelfth paragraph				
538	(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 <u>security</u> updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;	(7) in relation to the cybersecurity risks posed to the products with digital elements , provide for mechanisms to securely distribute updates for products with digital elements to ensure that ~~exploitable~~ vulnerabilities are fixed or mitigated in a timely and, where applicable, automatic manner;	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex I, thirteenth paragraph				
539	(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 are available to address identified security issues, they are disseminated without delay and <u>unless otherwise agreed between the parties in a business-to-business context</u> , 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 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.	
Annex I, thirteenth paragraph a				
539a		<u>(8a) where possible and applicable, notify the user of the end of the support period.</u>		
Annex II				
540	Annex II	Annex II	Annex II	Annex II Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex II, first paragraph				
541	INFORMATION AND INSTRUCTIONS TO THE USER	INFORMATION AND INSTRUCTIONS TO THE USER	INFORMATION AND INSTRUCTIONS TO THE USER	INFORMATION AND INSTRUCTIONS TO THE USER Text Origin: Commission Proposal
Annex II, second paragraph				
542	As a minimum, the product with digital elements shall be accompanied by:	As a minimum, the product with digital elements shall be accompanied by:	As a minimum, the product with digital elements shall be accompanied by:	As a minimum, the product with digital elements shall be accompanied by: Text Origin: Commission Proposal
Annex II, third paragraph				
543	1. the name, registered trade name or registered trade mark of the manufacturer, and the postal address and the email address at which the manufacturer can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product;	1. the name, registered trade name or registered trade mark of the manufacturer, and the postal address and the email address <u>and where available the website</u> at which the manufacturer can be contacted, on the product or, ~~where that is not possible,~~ on its packaging or in a document accompanying the product;	<i>deleted</i>	
Annex II, fourth paragraph				
544	2. the point of contact where information about cybersecurity vulnerabilities of the product can be	2. the point of <u>single</u> contact where information about cybersecurity vulnerabilities of the product can be	2. the single point of contact where information about ~~cybersecurity~~ vulnerabilities of the product with	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	reported and received;	reported and received <u>and the manufacturer's policy on coordinated vulnerabilities and where it can be found</u> ;	digital elements can be reported and received;	
Annex II, fifth paragraph				
545	3. the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;	3. the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;	3. ~~the correct identification of the type, batch, version or serial number or other element allowing the identification~~ Name and type and any additional information enabling the unique of the product ~~and the corresponding instructions and user information~~ ;	
Annex II, sixth paragraph				
546	4. the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;	4. the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;	4. the intended ~~use~~ purpose , including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;	
Annex II, seventh paragraph				
547	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Annex II, eighth paragraph				
548	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 <u>by the competent authorities in accordance with non-disclosure conditions set out in Article 52</u> ;	deleted	
Annex II, ninth paragraph				
549	7. where applicable, the internet address at which the EU declaration of conformity can be accessed;	7. where applicable, the internet address at which the EU declaration of conformity can be accessed;	deleted	
Annex II, tenth paragraph				
550	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, at the very least until when users can expect~~ <u>the support period during which users can expect vulnerabilities to be handled and</u> to receive security updates;	8. the type of technical security support offered by the manufacturer, expected product lifetime and end-date and until when the technical security support it will be provided, at the very least until when users can expect to receive security updates;	
Annex II, eleventh paragraph				
551	9. detailed instructions or an	9. detailed instructions or an	9. detailed instructions or, where	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	internet address referring to such detailed instructions and information on:	internet address referring to such detailed instructions and information on:	applicable , an internet address referring to such detailed instructions and information on:	
Annex II, eleventh paragraph, point (a)				
552	(a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;	(a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;	(a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;	(a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use; Text Origin: Commission Proposal
Annex II, eleventh paragraph, point (b)				
553	(b) how changes to the product can affect the security of data;	(b) how changes to the product can affect the security of data;	(b) how changes to the product can affect the security of data;	(b) how changes to the product can affect the security of data; Text Origin: Commission Proposal
Annex II, eleventh paragraph, point (c)				
554	(c) how security-relevant updates can be installed;	(c) how security-relevant updates can be installed;	(c) how security-relevant updates can be installed;	(c) how security-relevant updates can be installed; Text Origin: Commission Proposal
Annex II, eleventh paragraph, point (d)				
555	(d) the secure decommissioning of the product, including information on how user data can be securely	(d) the secure decommissioning of the product, including information on how user data can be securely	(d) the secure decommissioning of the product, including information on how user data can be securely	(d) the secure decommissioning of the product, including information on how user data can be securely

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	removed.	removed.	removed.	removed. Text Origin: Commission Proposal
Annex II, eleventh paragraph, point (e)				
555a			(e) how the default setting of automatically installed updates, as required by point (aaa) of section 1.3 of Annex I, can be turned off.	
Annex II, eleventh paragraph, point (da)				
555b				<u>(e) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential requirements in Annex I as well as documentation requirements in Annex V of this Regulation.</u>
Annex II, point 10.				
555c			10. If the manufacturer decides to make available the software bill of materials to the user, the information and instructions to the user accompanying the product with digital elements shall also include that software bill of materials as set out in Section 2,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			point (1) of Annex I.	
Annex III				
556	Annex III	Annex III	Annex III	Annex III Text Origin: Commission Proposal
Annex III, first paragraph				
557	CRITICAL PRODUCTS WITH DIGITAL ELEMENTS	CRITICAL PRODUCTS WITH DIGITAL ELEMENTS	~~CRITICAL CLASSES AND CATEGORIES OF~~ PRODUCTS WITH DIGITAL ELEMENTS	
Annex III, Part I				
558	Part I Class I	Part I Class I	Part I Class I	Part I Class I Text Origin: Commission Proposal
Annex III, first paragraph				
558a			Categories of products with digital elements which meet the criteria referred to in Article 6(1a), point (a):	
Annex III, point 1.				
559	1. Identity management systems software and privileged access	1. Identity management systems software and privileged access	<i>deleted</i>	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	management software;	management software;		
<i>Annex III, point 2.</i>				
560	2. Standalone and embedded browsers;	2. Standalone and embedded browsers;	<i>deleted</i>	
<i>Annex III, point 3.</i>				
561	3. Password managers;	3. Password managers;	<i>deleted</i>	
<i>Annex III, point 3a.</i>				
561a		<u>3a. Biometric readers;</u>		
<i>Annex III, point 4.</i>				
562	4. Software that searches for, removes, or quarantines malicious software;	4. Software that searches for, removes, or quarantines malicious software;	41. Software that searches for, removes, or quarantines malicious software;	
<i>Annex III, point 5.</i>				
563	5. Products with digital elements with the function of virtual private network (VPN);	5. Products with digital elements with the function of virtual private network (VPN);	<i>deleted</i>	
<i>Annex III, point 6.</i>				
564	6. Network management systems;	6. Network management systems;		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			<i>deleted</i>	
<i>Annex III, point 7.</i>				
565	7. Network configuration management tools;	7. Network configuration management tools;	<i>deleted</i>	
<i>Annex III, point 8.</i>				
566	8. Network traffic monitoring systems;	8. Network traffic monitoring systems;	<i>deleted</i>	
<i>Annex III, point 9.</i>				
567	9. Management of network resources;	9. Management of network resources;	<i>deleted</i>	
<i>Annex III, point 10.</i>				
568	10. Security information and event management (SIEM) systems;	10. Security information and event management (SIEM) systems;	<i>deleted</i>	
<i>Annex III, point 11.</i>				
569	11. Update/patch management, including boot managers;	11. Update/patch management, including boot managers;	~~11. Update/patch management, including boot managers;~~ General purpose boot managers;	
<i>Annex III, point 12.</i>				
570	12. Application configuration	12. Application configuration		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	management systems;	management systems;	<i>deleted</i>	
<i>Annex III, point 13.</i>				
571	13. Remote access/sharing software;	13. Remote ~~access/sharing~~ <u>access</u> software;	<i>deleted</i>	
<i>Annex III, point 14.</i>				
572	14. Mobile device management software;	14. Mobile device management software;	<i>deleted</i>	
<i>Annex III, second paragraph</i>				
572a			3. Public key infrastructure and digital certificate issuance software;	
<i>Annex III, third paragraph</i>				
572b			Categories of products with digital elements which meet the criteria referred to in Article 6(1a), point (b):	
<i>Annex III, point 15.</i>				
573	15. Physical network interfaces;	15. Physical <u>and virtual</u> network interfaces;	~~15~~ 1. Physical and virtual network interfaces;	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex III, point 16.				
574	16. Operating systems not covered by class II;	16. Operating systems not covered by class II;	~~162. General purpose~~ operating systems ~~not covered by class II;~~	
Annex III, point 17.				
575	17. Firewalls, intrusion detection and/or prevention systems not covered by class II;	17. Firewalls, intrusion detection and/or prevention systems not covered by class II;	<i>deleted</i>	
Annex III, point 18.				
576	18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;	<i>deleted</i>	~~183. Routers, modems intended for the connection to the internet, and switches, not covered by class II;~~	
Annex III, point 19.				
577	19. Microprocessors not covered by class II;	19. <u>General purpose microprocessors and</u> microprocessors not covered by class II;	~~194. Microprocessors not covered by class II;~~	
Annex III, point 20.				
578	20. Microcontrollers;	20. Microcontrollers;	~~205. Microcontrollers;~~	
Annex III, point 21.				
579	21. Application specific integrated circuits (ASIC) and field-	21. Application specific integrated circuits (ASIC) and field-	<i>deleted</i>	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];	programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in ~~[Annex I to the~~ Article 3 of Directive XXX/XXXX (NIS2 EU) ~~]~~ 2022/2555 ;		
Annex III, point 22.				
580	22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);	22. Industrial Automation & ~~amp;~~ Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC), industrial robots and their control systems and supervisory control and data acquisition systems (SCADA);	deleted	
Annex III, point 23.				
581	23. Industrial Internet of Things not covered by class II.	23. Industrial Internet of Things not covered by class II- ~~i~~ ;	deleted	
Annex III, point 24.				
581a		24. Home automation systems, including smart home servers and virtual assistants;		
Annex III, point 25.				
581b		25. Security devices, including		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<u>smart door locks, cameras and alarm systems;</u>		
Annex III, point 26.				
581c		<u>26. Smart toys;</u>		
Annex III, point 27.				
581d		<u>27. Personal health appliances and wearables.</u>		
Annex III, Part II				
582	Part II Class II	Part II Class II	Part II Class II	Part II Class II <u>Text Origin: Commission Proposal</u>
Annex III, Part II, first paragraph				
582a			Categories of products with digital elements which meet both criteria referred to in Article 6(2), points (a) and (b):	
Annex III, Part II, point 1.				
582b			1. Products with digital elements that support virtual private network (VPN) functions such as VPN server and clients;	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex III, point 24.				
583	24. Operating systems for servers, desktops, and mobile devices;	~~24~~ ¹ . Operating systems for servers, desktops, and mobile devices;	<i>deleted</i>	
Annex III, point 25.				
584	25. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;	~~25~~ ² . Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;	~~25~~ ² . Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;	~~25~~ ² . Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments; Text Origin: Commission Proposal
Annex III, point 26.				
585	26. Public key infrastructure and digital certificate issuers;	~~26~~ ³ . Public key infrastructure and digital certificate issuers;	<i>deleted</i>	
Annex III, point 27.				
586	27. Firewalls, intrusion detection and/or prevention systems intended for industrial use;	~~27~~ ⁴ . Firewalls, intrusion detection and/or prevention systems intended for industrial use;	~~27~~ ³ . Firewalls, intrusion detection and/or prevention systems intended for industrial use;.	
Annex III, point 28.				
587	28. General purpose microprocessors;	<i>deleted</i>	<i>deleted</i>	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
<i>Annex III, point 29.</i>				
588	29. Microprocessors intended for integration in programmable logic controllers and secure elements;	~~29~~ ⁶ . Microprocessors intended for integration in programmable logic controllers and secure elements;	deleted	
<i>Annex III, point 30.</i>				
589	30. Routers, modems intended for the connection to the internet, and switches, intended for industrial use;	~~30~~ ⁷ . Routers, modems intended for the connection to the internet, and switches, ~~intended for industrial use~~ ;	deleted	
<i>Annex III, point 31.</i>				
590	31. Secure elements;	~~31~~ ⁸ . Secure elements;	deleted	
<i>Annex III, point 32.</i>				
591	32. Hardware Security Modules (HSMs);	~~32~~ ⁹ . Hardware Security Modules (HSMs);	deleted	
<i>Annex III, point 33.</i>				
592	33. Secure cryptoprocessors;	~~33~~ ¹⁰ . Secure cryptoprocessors;	deleted	
<i>Annex III, point 34.</i>				
593	34. Smartcards, smartcard readers and tokens;	~~34~~ ¹¹ . Smartcards, smartcard readers and tokens;	deleted	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex III, point 35.				
594	35. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);	~~35~~ ¹² . Industrial Automation & ~~amp;~~ Control Systems (IACS) intended for the use by essential entities of the type referred to in ~~[Annex I to the~~ <u>Article 3 of</u> Directive ~~XXX/XXXX (NIS2EU)~~ <u>2022/2555</u> , such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);	deleted	
Annex III, point 36.				
595	36. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];	~~36~~ ¹³ . Industrial Internet of Things devices intended for the use by essential entities of the type referred to in ~~[Annex I to the~~ <u>Article 3 of</u> Directive ~~XXX/XXXX (NIS2EU)~~ <u>2022/2555</u> ;	deleted	
Annex III, point 37.				
596	37. Robot sensing and actuator components and robot controllers;	deleted	deleted	37. ~~Robot sensing and actuator components and robot controllers;~~ <u>deleted</u> Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex III, point 38.				
597	38. Smart meters.	~~38~~ ¹⁵ . Smart meters.	<i>deleted</i>	
Annex IIIa				
597a			Annex IIIa	
Annex IIIa				
597b			CATEGORIES OF PRODUCTS WITH DIGITAL ELEMENTS SUBJECT TO THE PROCEDURE PROVIDED FOR IN ARTICLE 6A	
Annex IIIa, point 1.				
597c			1. Hardware Devices with Security Boxes;	
Annex IIIa, point 2.				
597d			2. Smart meter gateways within smart metering systems as defined in Article 2 (23) of Directive (EU) 2019/944 and other devices for advanced security purposes, including for secure cryptoprocessing;	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex IIIa, point 3.				
597e			3. Smartcards or similar devices, including secure elements.	
Annex IIIb				
597f			Annex IIIb	
Annex IIIb				
597g			SIMPLIFIED EU DECLARATION OF CONFORMITY	
Annex IIIb, first paragraph				
597h			The simplified EU declaration of conformity referred to in Article [10(11)] shall be provided as follows:	
Annex IIIb, second paragraph				
597i			Hereby, [Name of manufacturer] declares that the product with digital elements type [designation of type of product with digital element] is in compliance with Regulation XX.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex IIIb, third paragraph				
597j			The full text of the EU declaration of conformity is available at the following internet address:	
Annex IV				
598	Annex IV	Annex IV	Annex IV	Annex IV Text Origin: Commission Proposal
Annex IV, first paragraph				
599	EU DECLARATION OF CONFORMITY	EU DECLARATION OF CONFORMITY	EU DECLARATION OF CONFORMITY	EU DECLARATION OF CONFORMITY Text Origin: Commission Proposal
Annex IV, second paragraph				
600	The EU declaration of conformity referred to in Article 20, shall contain all of the following information:	The EU declaration of conformity referred to in Article 20, shall contain all of the following information:	The EU declaration of conformity referred to in Article 20, shall contain all of the following information:	The EU declaration of conformity referred to in Article 20, shall contain all of the following information: Text Origin: Commission Proposal
Annex IV, third paragraph				
601				

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	1. Name and type and any additional information enabling the unique identification of the product with digital elements;	1. Name and type and any additional information enabling the unique identification of the product with digital elements;	1. Name and type and any additional information enabling the unique identification of the product with digital elements;	1. Name and type and any additional information enabling the unique identification of the product with digital elements; Text Origin: Commission Proposal
Annex IV, fourth paragraph				
602	2. Name and address of the manufacturer or his authorised representative;	2. Name and address of the manufacturer or his authorised representative;	2. Name and address of the manufacturer or his authorised representative;	2. Name and address of the manufacturer or his authorised representative; Text Origin: Commission Proposal
Annex IV, fifth paragraph				
603	3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;	3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;	3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;	3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider; Text Origin: Commission Proposal
Annex IV, sixth paragraph				
604	4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);	4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);	4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);	4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate); Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Annex IV, seventh paragraph			
605	5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;	5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;	5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;	5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation; Text Origin: Commission Proposal
	Annex IV, eighth paragraph			
606	6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;	6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;	6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;	6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared; Text Origin: Commission Proposal
	Annex IV, ninth paragraph			
607	7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;	7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;	7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;	7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex IV, eleventh paragraph				
608	8. Additional information:	8. Additional information:	8. Additional information:	8. Additional information: Text Origin: Commission Proposal
Annex IV, twelfth paragraph				
609	Signed for and on behalf of:.....	Signed for and on behalf of:.....	Signed for and on behalf of:.....	Signed for and on behalf of:..... Text Origin: Commission Proposal
Annex IV, thirteenth paragraph				
610	(place and date of issue):	(place and date of issue):	(place and date of issue):	(place and date of issue): Text Origin: Commission Proposal
Annex IV, fourteenth paragraph				
611	(name, function) (signature):	(name, function) (signature):	(name, function) (signature):	(name, function) (signature): Text Origin: Commission Proposal
Annex V				
612	Annex V	Annex V	Annex V	Annex V Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex V, first paragraph				
613	CONTENTS OF THE TECHNICAL DOCUMENTATION	CONTENTS OF THE TECHNICAL DOCUMENTATION	CONTENTS OF THE TECHNICAL DOCUMENTATION	CONTENTS OF THE TECHNICAL DOCUMENTATION Text Origin: Commission Proposal
Annex V, second paragraph				
614	The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements:	The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements:	The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements:	The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements: Text Origin: Commission Proposal
Annex V, third paragraph				
615	1. a general description of the product with digital elements, including:	1. a general description of the product with digital elements, including:	1. a general description of the product with digital elements, including:	1. a general description of the product with digital elements, including: Text Origin: Commission Proposal
Annex V, third paragraph, point (a)				
616	(a) its intended purpose;	(a) its intended purpose;	(a) its intended purpose;	(a) its intended purpose; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex V, third paragraph, point (b)				
617	(b) versions of software affecting compliance with essential requirements;	(b) versions of software affecting compliance with essential requirements;	(b) versions of software affecting compliance with essential requirements;	(b) versions of software affecting compliance with essential requirements; Text Origin: Commission Proposal
Annex V, third paragraph, point (c)				
618	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout; Text Origin: Commission Proposal
Annex V, third paragraph, point (d)				
619	(d) user information and instructions as set out in Annex II;	(d) user information and instructions as set out in Annex II;	(d) user information and instructions as set out in Annex II;	(d) user information and instructions as set out in Annex II; Text Origin: Commission Proposal
Annex V, fourth paragraph				
620	2. a description of the design, development and production of the product and vulnerability handling processes, including:	2. a description of the design, development and production of the product and vulnerability handling processes, including:	2. a description of the design, development and production of the product and vulnerability handling processes, including:	2. a description of the design, development and production of the product and vulnerability handling processes, including: Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Annex V, fourth paragraph, point (a)				
621	(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;	(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;	(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;	(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; Text Origin: Commission Proposal
Annex V, fourth paragraph, point (b)				
622	(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;	(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;	(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;	(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; Text Origin: Commission Proposal
Annex V, fourth paragraph, point (c)				

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
623	(c) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.	(c) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.	(c) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.	(c) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes. Text Origin: Commission Proposal
Annex V, fifth paragraph				
624	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. 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, <u>including how the essential requirements set out in Annex I, Section 1, are applicable</u> ;	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;	
Annex V, sixth paragraph				
625	4. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common	4. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common	4. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common	4. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied;	specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied;	specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied;	specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied; Text Origin: Commission Proposal
Annex V, seventh paragraph				
626	5. reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;	5. reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;	5. reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;	5. reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I; Text Origin: Commission Proposal
Annex V, eighth paragraph				
627	6. a copy of the EU declaration of conformity;	6. a copy of the EU declaration of conformity;	6. a copy of the EU declaration of conformity;	6. a copy of the EU declaration of conformity; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Annex V, ninth paragraph			
628	7. where applicable, the software bill of materials as defined in Article 3, point (36), 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.	7. where applicable, the software bill of materials as defined in Article 3, point (36), 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.	7. where applicable, the software bill of materials as defined in Article 3, point (36), 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.	7. where applicable, the software bill of materials as defined in Article 3, point (36), 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. Text Origin: Commission Proposal
	Annex VI			
629	Annex VI	Annex VI	Annex VI	Annex VI Text Origin: Commission Proposal
	Annex VI, first paragraph			
630	CONFORMITY ASSESSMENT PROCEDURES	CONFORMITY ASSESSMENT PROCEDURES	CONFORMITY ASSESSMENT PROCEDURES	CONFORMITY ASSESSMENT PROCEDURES Text Origin: Commission Proposal
	Annex VI, Part I			
631	Part I A. Conformity Assessment procedure based on internal control	Part I A. Conformity Assessment procedure based on internal control	Part I A. Conformity Assessment procedure based on internal control	Part I A. Conformity Assessment procedure based on internal control

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	(based on Module A)	(based on Module A)	(based on Module A)	(based on Module A) Text Origin: Commission Proposal
Annex VI, point 1.				
632	1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I.	1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I.	1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I.	1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I. Text Origin: Commission Proposal
Annex VI, point 2.				
633	2. The manufacturer shall draw up the technical documentation described in Annex V.	2. The manufacturer shall draw up the technical documentation described in Annex V.	2. The manufacturer shall draw up the technical documentation described in Annex V.	2. The manufacturer shall draw up the technical documentation described in Annex V. Text Origin: Commission Proposal
Annex VI, point 3., first subparagraph				
634	3. Design, development, production and vulnerability handling of	3. Design, development, production and vulnerability handling of	3. Design, development, production and vulnerability handling of	3. Design, development, production and vulnerability handling of

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	products with digital elements	products with digital elements	products with digital elements	products with digital elements Text Origin: Commission Proposal
Annex VI, point 3., second subparagraph				
635	The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I.	The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I.	The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I.	The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I. Text Origin: Commission Proposal
Annex VI, point 4.				
636	4. Conformity marking and declaration of conformity	4. Conformity marking and declaration of conformity	4. Conformity marking and declaration of conformity	4. Conformity marking and declaration of conformity Text Origin: Commission Proposal
Annex VI, second paragraph				
637	4.1. The manufacturer shall affix the CE to each individual product with digital elements that satisfies the applicable requirements of this	4.1. The manufacturer shall affix the CE to each individual product with digital elements that satisfies the applicable requirements of this	4.1. The manufacturer shall affix the CE to each individual product with digital elements that satisfies the applicable requirements of this	4.1. The manufacturer shall affix the CE to each individual product with digital elements that satisfies the applicable requirements of this

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Regulation.	Regulation.	Regulation.	Regulation. Text Origin: Commission Proposal
Annex VI, third paragraph				
638	4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.	4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market <u>or the support period, whichever is longer</u> . The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.	4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.	
Annex VI, point 5., first subparagraph				
639	5. Authorised representatives	5. Authorised representatives	5. Authorised representatives	5. Authorised representatives Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, point 5., second subparagraph				
640	The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate. Text Origin: Commission Proposal
Annex VI, Part II				
641	Part II B. EU-type examination (based on Module B)	Part II B. EU-type examination (based on Module B)	Part II ~~B~~ -EU-type examination (based on Module B)	
Annex VI, point 6.				
642	6. EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I.	~~6~~ <u>1</u> . EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I.	~~6~~ <u>1</u> . EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I.	~~6~~ <u>1</u> . EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, point 7.				
643	7. EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product through examination of the technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type).	~~7~~ 2. EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product through examination of the technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type).	~~7~~ 2. EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product through examination of the technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type).	~~7~~ 2. EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product through examination of the technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type). Text Origin: Commission Proposal
Annex VI, point 8., first subparagraph				
644	3. The manufacturer shall lodge an application for EU-type examination with a single notified body of his choice.	3. The manufacturer shall lodge an application for EU-type examination with a single notified body of his choice.	3. The manufacturer shall lodge an application for EU-type examination with a single notified body of his choice.	3. The manufacturer shall lodge an application for EU-type examination with a single notified body of his choice. Text Origin: Commission Proposal
Annex VI, point 8., second subparagraph				
645	The application shall include:	The application shall include:	The application shall include:	The application shall include: Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, fourth paragraph				
646	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well; Text Origin: Commission Proposal
Annex VI, fifth paragraph				
647	- a written declaration that the same application has not been lodged with any other notified body;	- a written declaration that the same application has not been lodged with any other notified body;	- a written declaration that the same application has not been lodged with any other notified body;	- a written declaration that the same application has not been lodged with any other notified body; Text Origin: Commission Proposal
Annex VI, sixth paragraph				
648	- the technical documentation, which shall make it possible to assess the product's conformity with the applicable essential requirements as set out in Section 1 of Annex I and the manufacturer's vulnerability handling processes set out in Section 2 of Annex I, and shall include an adequate analysis and assessment of the risk(s). The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and	- the technical documentation, which shall make it possible to assess the product's conformity with the applicable essential requirements as set out in Section 1 of Annex I and the manufacturer's vulnerability handling processes set out in Section 2 of Annex I, and shall include an adequate analysis and assessment of the risk(s). The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and	- the technical documentation, which shall make it possible to assess the product's conformity with the applicable essential requirements as set out in Section 1 of Annex I and the manufacturer's vulnerability handling processes set out in Section 2 of Annex I, and shall include an adequate analysis and assessment of the risk(s). The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and	- the technical documentation, which shall make it possible to assess the product's conformity with the applicable essential requirements as set out in Section 1 of Annex I and the manufacturer's vulnerability handling processes set out in Section 2 of Annex I, and shall include an adequate analysis and assessment of the risk(s). The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	operation of the product. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex V;	operation of the product. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex V;	operation of the product. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex V;	operation of the product. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex V; Text Origin: Commission Proposal
Annex VI, seventh paragraph				
649	- the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards and/or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under his responsibility.	- the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards and/or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under his responsibility.	- the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards and/or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under his responsibility.	- the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards and/or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under his responsibility. Text Origin: Commission Proposal
Annex VI, point 9.				
650	9. The notified body shall:	~~9~~ 4. The notified body shall:	94. The notified body shall:	~~9~~ 4. The notified body shall: Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, eighth paragraph				
651	4.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with the essential requirements set out in Section 1 of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I;	4.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with the essential requirements set out in Section 1 of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I;	4.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with the essential requirements set out in Section 1 of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I;	4.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with the essential requirements set out in Section 1 of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I; Text Origin: Commission Proposal
Annex VI, ninth paragraph				
652	4.2. verify that the specimen(s) have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards and/or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;	4.2. verify that the specimen(s) have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards and/or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;	4.2. verify that the specimen(s) have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards and/or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;	4.2. verify that the specimen(s) have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards and/or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, tenth paragraph				
653	4.3. carry out appropriate examinations and tests, or have them carried out, to check whether, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I, these have been applied correctly;	4.3. carry out appropriate examinations and tests, or have them carried out, to check whether, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I, these have been applied correctly;	4.3. carry out appropriate examinations and tests, or have them carried out, to check whether, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I, these have been applied correctly;	4.3. carry out appropriate examinations and tests, or have them carried out, to check whether, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I, these have been applied correctly; Text Origin: Commission Proposal
Annex VI, eleventh paragraph				
654	4.4. carry out appropriate examinations and tests, or have them carried out, to check whether, where the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential requirements;	4.4. carry out appropriate examinations and tests, or have them carried out, to check whether, where the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential requirements;	4.4. carry out appropriate examinations and tests, or have them carried out, to check whether, where the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential requirements;	4.4. carry out appropriate examinations and tests, or have them carried out, to check whether, where the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential requirements; Text Origin: Commission Proposal
Annex VI, twelfth paragraph				
655	4.5. agree with the manufacturer on a location where the examinations	4.5. agree with the manufacturer on a location where the examinations	4.5. agree with the manufacturer on a location where the examinations	4.5. agree with the manufacturer on a location where the examinations

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	and tests will be carried out.	and tests will be carried out.	and tests will be carried out.	and tests will be carried out. Text Origin: Commission Proposal
Annex VI, point 10.				
656	10. The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.	~~105.~~ The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.	~~105.~~ The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.	~~105.~~ The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer. Text Origin: Commission Proposal
Annex VI, point 11., first subparagraph				
657	6. Where the type and the vulnerability handling processes meet the essential requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes.	6. Where the type and the vulnerability handling processes meet the essential requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes.	6. Where the type and the vulnerability handling processes meet the essential requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes.	6. Where the type and the vulnerability handling processes meet the essential requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	The certificate may have one or more annexes attached.	The certificate may have one or more annexes attached.	The certificate may have one or more annexes attached.	The certificate may have one or more annexes attached. Text Origin: Commission Proposal
Annex VI, point 11., second subparagraph				
658	The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.	The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.	The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.	The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control. Text Origin: Commission Proposal
Annex VI, point 11., third subparagraph				
659	Where the type and the vulnerability handling processes do not satisfy the applicable essential requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.	Where the type and the vulnerability handling processes do not satisfy the applicable essential requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.	Where the type and the vulnerability handling processes do not satisfy the applicable essential requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.	Where the type and the vulnerability handling processes do not satisfy the applicable essential requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, point 12., first subparagraph				
660	7. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.	7. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.	7. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.	7. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly. Text Origin: Commission Proposal
Annex VI, point 12., second subparagraph				
661	The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.	The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.	The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.	The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate. Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Annex VI, point 13., first subparagraph				
662	8. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted.	8. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted.	8. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted.	8. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted. Text Origin: Commission Proposal
Annex VI, point 13., second subparagraph				
663	Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued.	Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued.	Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued.	Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, point 13., third subparagraph				
664	The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and/or additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.	The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and/or additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.	The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and/or additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.	The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and/or additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate. Text Origin: Commission Proposal
Annex VI, point 14.				
665	14. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market.	~~14~~ 9. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market <u>or for the support period</u> .	~~14~~ 9. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, point 15.				
666	15. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 9, provided that they are specified in the mandate.	~~15~~ 10. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 9, provided that they are specified in the mandate.	~~15~~ 10. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 9, provided that they are specified in the mandate.	~~15~~ 10. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 9, provided that they are specified in the mandate. Text Origin: Commission Proposal
Annex VI, Part III				
667	Part III C. Conformity to type based on internal production control (based on Module C)	Part III C. Conformity to type based on internal production control (based on Module C)	Part III ~~C~~ . Conformity to type based on internal production control (based on Module C)	
Annex VI, point 16.				
668	16. Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 3, and ensures and declares that the products concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential requirements set out in Section 1 of Annex I.	~~16~~ 1. Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 3, and ensures and declares that the products concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential requirements set out in Section 1 of Annex I.	~~16~~ 1. Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 3, and ensures and declares that the products concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Annex VI, point 17.			
669	17. Production	~~17~~ 2. Production	~~17~~ 2. Production	~~17~~ 2. Production Text Origin: Commission Proposal
	Annex VI, thirteenth paragraph			
670	2.1. The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with the approved type described in the EU-type examination certificate and with the essential requirements as set out in Section 1 of Annex I.	2.1. The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with the approved type described in the EU-type examination certificate and with the essential requirements as set out in Section 1 of Annex I.	2.1. The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with the approved type described in the EU-type examination certificate and with the essential requirements as set out in Section 1 of Annex I and ensures that the manufacturer meets the essential requirements set out in Section 2 of Annex I.	
	Annex VI, point 18.			
671	18. Conformity marking and declaration of conformity	~~18~~ 3. Conformity marking and declaration of conformity	~~18~~ 3. Conformity marking and declaration of conformity	~~18~~ 3. Conformity marking and declaration of conformity Text Origin: Commission Proposal
	Annex VI, fourteenth paragraph			
672	3.1. The manufacturer shall affix the	3.1. The manufacturer shall affix the	3.1. The manufacturer shall affix the	3.1. The manufacturer shall affix the

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	CE marking to each individual product that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements of the legislative instrument.	CE marking to each individual product that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements of the legislative instrument.	CE marking to each individual product that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements of the legislative instrument.	CE marking to each individual product that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements of the legislative instrument. Text Origin: Commission Proposal
Annex VI, fifteenth paragraph				
673	3.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	3.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market <u>or for the support period</u> . The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	3.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	
Annex VI, point 19., first subparagraph				
674	4. Authorised representative	4. Authorised representative	4. Authorised representative	4. Authorised representative Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, point 19., second subparagraph				
675	The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate. Text Origin: Commission Proposal
Annex VI, Part IV				
676	Part IV H. Conformity based on full quality assurance (based on Module H)	Part IV H. Conformity based on full quality assurance (based on Module H)	Part IV ~~H~~ . Conformity based on full quality assurance (based on Module H)	
Annex VI, point 20.				
677	20. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5, and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I.	~~20~~ 1. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5, and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I.	~~20~~ 1. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5, and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I.	~~20~~ 1. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5, and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I. Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Annex VI, point 21., first subparagraph				
678	2. Design, development, production and vulnerability handling of products with digital elements	2. Design, development, production and vulnerability handling of products with digital elements	2. Design, development, production and vulnerability handling of products with digital elements	2. Design, development, production and vulnerability handling of products with digital elements Text Origin: Commission Proposal
Annex VI, point 21., second subparagraph				
679	The manufacturer shall operate an approved quality system as specified in point 3 for the design, development, and production of the products concerned and for handling vulnerabilities, maintain its effectiveness throughout the lifecycle of the products concerned, and shall be subject to surveillance as specified in point 4.	The manufacturer shall operate an approved quality system as specified in point 3 for the design, development, and production of the products concerned and for handling vulnerabilities, maintain its effectiveness throughout the lifecycle of the products concerned, and shall be subject to surveillance as specified in point 4.	The manufacturer shall operate an approved quality system as specified in point 3 for the design, development, and production of the products concerned and for handling vulnerabilities, maintain its effectiveness throughout the lifecycle of the products concerned, and shall be subject to surveillance as specified in point 4.	The manufacturer shall operate an approved quality system as specified in point 3 for the design, development, and production of the products concerned and for handling vulnerabilities, maintain its effectiveness throughout the lifecycle of the products concerned, and shall be subject to surveillance as specified in point 4. Text Origin: Commission Proposal
Annex VI, point 22.				
680	22. Quality system	~~22~~ 3. Quality system	~~22~~ 3. Quality system	~~22~~ 3. Quality system Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, seventeenth paragraph				
681	3.1. The manufacturer shall lodge an application for assessment of his quality system with the notified body of his choice, for the products concerned.	3.1. The manufacturer shall lodge an application for assessment of his quality system with the notified body of his choice, for the products concerned.	3.1. The manufacturer shall lodge an application for assessment of his quality system with the notified body of his choice, for the products concerned.	3.1. The manufacturer shall lodge an application for assessment of his quality system with the notified body of his choice, for the products concerned. Text Origin: Commission Proposal
Annex VI, eighteenth paragraph				
682	The application shall include:	The application shall include:	The application shall include:	The application shall include: Text Origin: Commission Proposal
Annex VI, nineteenth paragraph				
683	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;	- the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well; Text Origin: Commission Proposal
Annex VI, twentieth paragraph				
684	- the technical documentation for one model of each category of products intended to be manufactured or developed. The	- the technical documentation for one model of each category of products intended to be manufactured or developed. The	- the technical documentation for one model of each category of products intended to be manufactured or developed. The	- the technical documentation for one model of each category of products intended to be manufactured or developed. The

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	technical documentation shall, wherever applicable, contain at least the elements as set out in Annex V;	technical documentation shall, wherever applicable, contain at least the elements as set out in Annex V;	technical documentation shall, wherever applicable, contain at least the elements as set out in Annex V;	technical documentation shall, wherever applicable, contain at least the elements as set out in Annex V; Text Origin: Commission Proposal
Annex VI, twenty-first paragraph				
685	- the documentation concerning the quality system; and	- the documentation concerning the quality system; and	- the documentation concerning the quality system; and	- the documentation concerning the quality system; and Text Origin: Commission Proposal
Annex VI, twenty-second paragraph				
686	- a written declaration that the same application has not been lodged with any other notified body.	- a written declaration that the same application has not been lodged with any other notified body.	- a written declaration that the same application has not been lodged with any other notified body.	- a written declaration that the same application has not been lodged with any other notified body. Text Origin: Commission Proposal
Annex VI, twenty-fourth paragraph				
687	3.2. The quality system shall ensure compliance of the products with the essential requirements set out in Section 1 of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Section 2 of Annex I.	3.2. The quality system shall ensure compliance of the products with the essential requirements set out in Section 1 of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Section 2 of Annex I.	3.2. The quality system shall ensure compliance of the products with the essential requirements set out in Section 1 of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Section 2 of Annex I.	3.2. The quality system shall ensure compliance of the products with the essential requirements set out in Section 1 of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Section 2 of Annex I. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Annex VI, twenty-fifth paragraph				
688	All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.	All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.	All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.	All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records. Text Origin: Commission Proposal
Annex VI, twenty-sixth paragraph				
689	It shall, in particular, contain an adequate description of:	It shall, in particular, contain an adequate description of:	It shall, in particular, contain an adequate description of:	It shall, in particular, contain an adequate description of: Text Origin: Commission Proposal
Annex VI, twenty-seventh paragraph				
690	- the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;	- the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;	- the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;	- the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling; Text Origin: Commission

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Annex VI, twenty-eighth paragraph				
691	- the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 1 of Annex I that apply to the products will be met;	- the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 1 of Annex I that apply to the products will be met;	- the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 1 of Annex I that apply to the products will be met;	- the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 1 of Annex I that apply to the products will be met; Text Origin: Commission Proposal
Annex VI, twenty-ninth paragraph				
692	- the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 2 of Annex I that apply to the manufacturer will be met;	- the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 2 of Annex I that apply to the manufacturer will be met;	- the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 2 of Annex I that apply to the manufacturer will be met;	- the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 2 of Annex I that apply to the manufacturer will be met; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, thirtieth paragraph				
693	- the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products pertaining to the product category covered;	- the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products pertaining to the product category covered;	- the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products pertaining to the product category covered;	- the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products pertaining to the product category covered; Text Origin: Commission Proposal
Annex VI, thirty-first paragraph				
694	- the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;	- the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;	- the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;	- the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used; Text Origin: Commission Proposal
Annex VI, thirty-second paragraph				
695	- the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;	- the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;	- the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;	- the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out; Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, thirty-third paragraph				
696	- the quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc;	- the quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc;	- the quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc;	- the quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc; Text Origin: Commission Proposal
Annex VI, thirty-fourth paragraph				
697	- the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.	- the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.	- the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.	- the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system. Text Origin: Commission Proposal
Annex VI, thirty-sixth paragraph				
698	3.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.	3.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.	3.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.	3.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2. Text Origin: Commission Proposal
Annex VI, thirty-seventh paragraph				
699	It shall presume conformity with those requirements in respect of the elements of the quality system that	It shall presume conformity with those requirements in respect of the elements of the quality system that	It shall presume conformity with those requirements in respect of the elements of the quality system that	It shall presume conformity with those requirements in respect of the elements of the quality system that

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification.	comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification.	comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification.	comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification. Text Origin: Commission Proposal
Annex VI, thirty-eighth paragraph				
700	In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and knowledge of the applicable requirements of this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1, second indent, to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with those requirements.	In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and knowledge of the applicable requirements of this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1, second indent, to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with those requirements.	In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and knowledge of the applicable requirements of this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1, second indent, to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with those requirements.	In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and knowledge of the applicable requirements of this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1, second indent, to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with those requirements. Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VI, thirty-ninth paragraph				
701	The manufacturer or his authorised representative shall be notified of the decision.	The manufacturer or his authorised representative shall be notified of the decision.	The manufacturer or his authorised representative shall be notified of the decision.	The manufacturer or his authorised representative shall be notified of the decision. Text Origin: Commission Proposal
Annex VI, fortieth paragraph				
702	The notification shall contain the conclusions of the audit and the reasoned assessment decision.	The notification shall contain the conclusions of the audit and the reasoned assessment decision.	The notification shall contain the conclusions of the audit and the reasoned assessment decision.	The notification shall contain the conclusions of the audit and the reasoned assessment decision. Text Origin: Commission Proposal
Annex VI, forty-first paragraph				
703	3.4. The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.	3.4. The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.	3.4. The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.	3.4. The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient. Text Origin: Commission Proposal
Annex VI, forty-third paragraph				
704	3.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality	3.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality	3.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality	3.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	system.	system.	system.	system. Text Origin: Commission Proposal
Annex VI, forty-fourth paragraph				
705	The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.	The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.	The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.	The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary. Text Origin: Commission Proposal
Annex VI, forty-fifth paragraph				
706	It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.	It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.	It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.	It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision. Text Origin: Commission Proposal
Annex VI, point 23.				
707	23. Surveillance under the responsibility of the notified body	~~23~~ 4. Surveillance under the responsibility of the notified body	~~23~~ 4. Surveillance under the responsibility of the notified body	~~23~~ 4. Surveillance under the responsibility of the notified body Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Annex VI, forty-sixth paragraph			
708	4.1. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.	4.1. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.	4.1. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.	4.1. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system. Text Origin: Commission Proposal
	Annex VI, forty-seventh paragraph			
709	4.2. The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:	4.2. The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:	4.2. The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:	4.2. The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular: Text Origin: Commission Proposal
	Annex VI, forty-eighth paragraph			
710	- the quality system documentation;	- the quality system documentation;	- the quality system documentation;	- the quality system documentation; Text Origin: Commission Proposal
	Annex VI, forty-ninth paragraph			
711	- the quality records as provided for by the design part of the quality	- the quality records as provided for by the design part of the quality	- the quality records as provided for by the design part of the quality	- the quality records as provided for by the design part of the quality

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	system, such as results of analyses, calculations, tests, etc.;	system, such as results of analyses, calculations, tests, etc.;	system, such as results of analyses, calculations, tests, etc.;	system, such as results of analyses, calculations, tests, etc.;
				Text Origin: Commission Proposal
Annex VI, fiftieth paragraph				
712	- the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.	- the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.	- the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.	- the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.
				Text Origin: Commission Proposal
Annex VI, fifty-first paragraph				
713	4.3. The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.	4.3. The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.	4.3. The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.	4.3. The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.
				Text Origin: Commission Proposal
Annex VI, point 24.				
714	24. Conformity marking and declaration of conformity	~~24~~ 5. Conformity marking and declaration of conformity	~~24~~ 5. Conformity marking and declaration of conformity	~~24~~ 5. Conformity marking and declaration of conformity
				Text Origin: Commission Proposal

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Proposal
Annex VI, fifty-second paragraph				
715	5.1. The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product that satisfies the requirements set out in Section 1 of Annex I to this Regulation.	5.1. The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product that satisfies the requirements set out in Section 1 of Annex I to this Regulation.	5.1. The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product that satisfies the requirements set out in Section 1 of Annex I to this Regulation.	5.1. The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product that satisfies the requirements set out in Section 1 of Annex I to this Regulation. Text Origin: Commission Proposal
Annex VI, fifty-fourth paragraph				
716	5.2. The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up.	5.2. The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market <u>or for the support period</u> . The declaration of conformity shall identify the product model for which it has been drawn up.	5.2. The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up.	
Annex VI, fifty-fifth paragraph				
717	A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Annex VI, point 25.				
718	25. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market, keep at the disposal of the national authorities:	~~25~~ 6. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market <u>or for the support period or the period during which vulnerabilities are handled</u> , keep at the disposal of the national authorities:	~~25~~ 6. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market, keep at the disposal of the national authorities:	
Annex VI, fifty-sixth paragraph				
719	- the technical documentation referred to in point 3.1;	- the technical documentation referred to in point 3.1;	- the technical documentation referred to in point 3.1;	- the technical documentation referred to in point 3.1; Text Origin: Commission Proposal
Annex VI, fifty-seventh paragraph				
720	- the documentation concerning the quality system referred to in point 3.1;	- the documentation concerning the quality system referred to in point 3.1;	- the documentation concerning the quality system referred to in point 3.1;	- the documentation concerning the quality system referred to in point 3.1; Text Origin: Commission Proposal
Annex VI, fifty-eighth paragraph				
721	- the change referred to in point 3.5,	- the change referred to in point 3.5,	- the change referred to in point 3.5,	- the change referred to in point 3.5,

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	as approved;	as approved;	as approved;	as approved; Text Origin: Commission Proposal
Annex VI, fifty-ninth paragraph				
722	- the decisions and reports of the notified body referred to in points 3.5, 4.3 and 4.4.	- the decisions and reports of the notified body referred to in points 3.5, 4.3 and 4.4.	- the decisions and reports of the notified body referred to in points 3.5, 4.3 and 4.4.	- the decisions and reports of the notified body referred to in points 3.5, 4.3 and 4.4. Text Origin: Commission Proposal
Annex VI, point 26., first subparagraph				
723	7. Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.	7. Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.	7. Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.	7. Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted. Text Origin: Commission Proposal
Annex VI, point 26., second subparagraph				
724	Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.	Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.	Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.	Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Annex VI, point 27., first subparagraph				
725	8. Authorised representative	8. Authorised representative	8. Authorised representative	8. Authorised representative Text Origin: Commission Proposal
Annex VI, point 27., second subparagraph				
726	The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate. Text Origin: Commission Proposal
Annex VIa				
726a		<u>Annex VIa</u>		
Annex VIa, first paragraph				
726b		<u>CAPACITY NEEDS OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)</u>		

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Annex VIa, second paragraph				
726c		<u><i>In order to fulfil its obligations under this Regulation and in order not to compromise existing obligations of the Agency under other Union law, the adequate staffing and financing of ENISA shall be ensured. Therefore additional tasks for ENISA under this Regulation shall be accompanied by additional human and financial resources. Nine additional full-time equivalent and corresponding additional appropriations will be needed to cover the additional tasks under this Regulation.</i></u>		