**TABLE OF CONCORDANCE**

| | | | | | | |
|---|---|---|---|---|---|---|
| **REGULATION (EU) 2024/2847** of the European Parliament and of the council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)<br><br>**Nr. CELEX:** EUR-Lex- 32024R2847<br>**Nr. Natyral:** 2024/2847/BE<br>**Fletore Zyrtare:** Seria L, 2024/2847, 20.11.2024 | | **The draft** law "On cybersecurity requirements for products with digital elements and cyber resilience," which is aligned with Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828, Nr. CELEX: EUR-Lex-32024R2847, Nr. Natyral: 2024/2847/BE, Fletore Zyrtare: Seria L, 2024/2847, 20.11.2024<br><br>**Level of alignment**<br>**F –** Full alignment<br>**P –** Partial alignment<br>**N –** Non alignment | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **Article** | **Text** | **Reference** | **Article** | **Content** | **Compliance** | **Notes** |
| *This column indicates only the article number, paragraph, or subparagraph of the EU acquis instrument.* | *This column indicates only the article number, paragraph, or subparagraph of the EU acquis instrument.* | *If there is more than one national legal act transposing it, they are numbered and the corresponding reference number is entered in this column, in accordance with the order at the top of the table (*).* | *This column indicates the article number of the law or national act.* | *This column shows the text of the article, or parts thereof, corresponding to the number in the fourth column, which has been aligned with the requirements of the EU acquis article listed in the second column.* | *This column shows the degree of approximation for each specific article.* | *This column provides information on the degree of approximation. Where approximation is not complete, the reasons and the timelines for achieving full approximation are provided.* |

| Article | Text | Reference | Article | Content | Compliance | Notes |
|---|---|---|---|---|---|---|
| **A1** | Article 1<br>**Subject matter**<br><br>This Regulation lays down:<br>(a) rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products;<br>(b) essential cybersecurity requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;<br>(c) essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the products are expected to be in use, and obligations for economic operators in relation to those processes;<br>(d) rules on market surveillance, including monitoring, and enforcement of the rules and requirements referred to in this Article. | | **A1** | Article 1<br>**Subject matter**<br><br>This law lays down:<br>a) rules for placing products with digital elements on the market, in order to ensure the cybersecurity of those products;<br>b) essential cybersecurity requirements for the design, development and production of products with digital elements, as well as the obligations of economic operators in relation to those products as regards cybersecurity;<br>c) essential cybersecurity requirements for vulnerability-handling processes established by manufacturers to ensure the cybersecurity of products with digital elements during their expected period of use, as well as the obligations of economic operators in relation to those processes;<br>ç) rules on market surveillance, including monitoring and enforcement of the requirements laid down in this article. | **F** | |
| **A2** | Article 2<br>**Scope**<br><br>1. This Regulation applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.<br>2. This Regulation does not apply to products with digital elements to which the following Union legal acts apply:<br>(a) Regulation (EU) 2017/745;<br>(b) Regulation (EU) 2017/746;<br>(c) Regulation (EU) 2019/2144.<br>3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.<br>4. This Regulation does not apply to equipment that falls within the scope of Directive 2014/90/EU of the European Parliament and of the Council (36).<br>5. 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 cybersecurity requirements set out in Annex I may be limited or excluded where:<br><br>(a) such limitation or exclusion is consistent with the | | **A2** | Article 2<br>**Scope**<br><br>1. This law shall apply to products with digital elements made available on the market whose intended purpose includes a direct or indirect, logical or physical, data connection to a device or network.<br>2. This law shall not apply to products with digital elements regulated by the legislation in force as follows:<br>a) medical devices pursuant to law no. 89/2014 “On Medical Devices’;<br>b) *in vitro* medical devices pursuant to law no. 89/2014 “On Medical Devices’;<br>c) motor vehicles and their trailers, as well as the systems, components and separate technical units intended for such vehicles, pursuant to the legislation in force on type-approval requirements concerning their general safety and the protection of vehicle occupants and vulnerable road users.<br>3. This law shall not apply to products with digital elements in the field of civil aviation that are subject to the rules on essential requirements in the field of civil aviation under the legislation in force adopted in accordance with European Union practice. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | overall regulatory framework that applies to those products; and<br>(b) the sectoral rules achieve the same or a higher level of protection as that provided for by this Regulation.<br>The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by specifying whether such limitation or exclusion is necessary, the products and rules concerned, as well as the scope of the limitation, if relevant.<br>6. This Regulation does not apply to spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace.<br>7. This Regulation does not apply to products with digital elements developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information.<br>8. 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. | | | 4. This law shall not apply to marine equipment subject to specific legal rules on safety at sea requirements in accordance with European Union practice and the international conventions to which Albania is a party.<br>5. The application of this law may be restricted or excluded in relation to products with digital elements that are subject to other relevant legislation in force laying down requirements relating to all or some of the risks covered by the essential cybersecurity requirements set out in annex I to this law, where:<br>a) such a restriction or exclusion is consistent with the overall regulatory framework applicable to those products; and<br>b) the sectoral rules achieve the same or a higher level of protection than this law.<br>Where necessary, the cases in which the application of this law is restricted or excluded under this point, the products concerned, the relevant rules and the scope of the restriction, as applicable, shall be approved by decision of the Council of Ministers.<br>6. This law shall not apply to spare parts made available on the market to replace identical components in products with digital elements, where those spare parts are manufactured to the same specifications as the components they are intended to replace.<br>7. This law shall not apply to products with digital elements developed or modified exclusively for national security or defence purposes, or to products specifically designed for processing classified information.<br>8. The obligations laid down in this law shall not include the provision of information where its disclosure would be contrary to the essential interests of the national security, public security or defence of the Republic of Albania. | | |
| **A3** | Article 3<br>**Definitions**<br><br>For the purposes of this Regulation, the following definitions apply: | | **A3** | Article 3<br>**Definitions**<br><br>For the purposes of this law, the following definitions shall apply: | **F** | |
| **A3, point 1** | (1) 'product with digital elements' means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately; | | **A3, point 1** | 1. "Product with digital elements" means a software or hardware product and its remote data processing solutions, including software or hardware components placed on the market separately. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A3, point 2** | (2) 'remote data processing' means 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; | | **A3, point 2** | 2. "Remote data processing" means data processing at a distance for which the software is designed and developed by the manufacturer or under its responsibility, and without which the product with digital elements would be unable to perform one of its functions. | **F** | |
| **A3, point 3** | (3) 'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881; | | **A3, point 3** | 3. "Cybersecurity" has the same meaning as in law No. 25/2024 "On Cybersecurity". | **F** | |
| **A3, point 4** | (4) 'software' means the part of an electronic information system which consists of computer code; | | **A3, point 4** | 4. "Software" means the part of an electronic information system consisting of computer code. | **F** | |
| **A3, point 5** | (5) 'hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data; | | **A3, point 5** | 5. "Hardware" means a physical electronic information system or parts thereof capable of processing, storing or transmitting digital data. | **F** | |
| **A3, point 6** | (6) 'component' means software or hardware intended for integration into an electronic information system; | | **A3, point 6** | 6. "Component" means software or hardware intended to be integrated into an electronic information system. | **F** | |
| **A3, point 7** | (7) 'electronic information system' means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data; | | **A3, point 7** | 7. "Electronic information system" means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data. | **F** | |
| **A3, point 8** | (8) 'logical connection' means a virtual representation of a data connection implemented through a software interface; | | **A3, point 8** | 8. "Logical connection" means a virtual representation of a data connection implemented through a software interface. | **F** | |
| **A3, point 9** | (9) 'physical connection' means a connection between electronic information systems or components implemented using physical means, including through electrical, optical or mechanical interfaces, wires or radio waves; | | **A3, point 9** | 9. "Physical connection" means a connection between electronic information systems or components implemented by physical means, including electrical, optical or mechanical interfaces, wires or radio waves. | **F** | |
| **A3, point 10** | (10) '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; | | **A3, point 10** | 10. "Indirect connection" means a connection to a device or network that does not occur directly, but is implemented through a larger system that is directly connected to it. | **F** | |
| **A3, point 11** | (11) 'end-point' means any device that is connected to a network and serves as an entry point to that network; | | **A3, point 11** | 11. "Endpoint" means any device connected to a network that serves as an entry point to that network. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A3, point 12** | (12) 'economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations in relation to the manufacture of products with digital elements or to the making available of products with digital elements on the market in accordance with this Regulation; | | **A3, point 12** | 12. "Economic operator" means the manufacturer, authorised representative, importer, distributor or any other natural or legal person that has obligations in relation to the manufacture or making available on the market of products with digital elements, as provided for in this law. | **F** | |
| **A3, point 13** | (13) 'manufacturer' means a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge; | | **A3, point 13** | 13. "Manufacturer" means any natural or legal person who develops or manufactures, or has a product with digital elements designed or manufactured, and markets that product under its name or trademark, whether for payment, for profit or free of charge. | **F** | |
| **A3, point 14** | (14) 'open-source software steward' means a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products; | | **A3, point 14** | 14. "Open-source software steward" means a legal person, other than the manufacturer, whose purpose is to provide sustained support for the development of products with digital elements that qualify as free and open-source software and are intended for commercial activities, and to ensure their viability. | **F** | |
| **A3, point 15** | (15) 'authorised representative' means a natural or legal person established within the Union who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks; | | **A3, point 15** | 15. "Authorised representative" means a natural or legal person established in the Republic of Albania that has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks. | **F** | |
| **A3, point 16** | (16) 'importer' means a 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; | | **A3, point 16** | 16. "Importer" means a natural or legal person established in the Republic of Albania that places on the market a product with digital elements bearing the name or trademark of a natural or legal person established outside the Republic of Albania. | **F** | |
| **A3, point 17** | (17) 'distributor' means a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties; | | **A3, point 17** | 17. "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 market without affecting its properties. | **F** | |
| **A3, point 18** | (18) 'consumer' means a natural person who acts for purposes which are outside that person's trade, business, craft or profession; | | **A3, point 18** | 18. "Consumer" means any natural person acting for purposes outside that person"s trade, business, craft or profession; it has the same meaning as under law No. 9902 of 17 April 2008 "On Consumer Protection", as amended. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A3, point 19** | (19) 'microenterprises', 'small enterprises' and 'medium-sized enterprises' mean, respectively, microenterprises, small enterprises and medium-sized enterprises as defined in the Annex to Recommendation 2003/361/EC; | | **A3, point 19** | 19. "Microenterprise, small enterprise and medium-sized enterprise" have the same meaning as in law No. 43/2022 "On the Development of Micro, Small and Medium-Sized Enterprises". | **F** | |
| **A3, point 20** | (20) 'support period' means the period during which a manufacturer is required to ensure that vulnerabilities of a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I; | | **A3, point 20** | 20. "Support period" means the period during which a manufacturer is required to ensure that vulnerabilities in a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in part II of annex I to this law. | **F** | |
| **A3, point 21** | (21) 'placing on the market' means the first making available of a product with digital elements on the Union market; | | **A3, point 21** | 21. "Placing on the market" means the first making available of a product with digital elements on the market. | **F** | |
| **A3, point 22** | (22) 'making available on the market' means the 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; | | **A3, point 22** | 22. "Making available on the market" means any supply of a product with digital elements for distribution, consumption or use on the market in the course of a commercial activity, whether in return for payment or free of charge. | **F** | |
| **A3, point 23** | (23) '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; | | **A3, point 23** | 23. "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, and in the technical documentation. | **F** | |
| **A3, point 24** | (24) '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; | | **A3, point 24** | 24. "Reasonably foreseeable use" means use that is not necessarily the intended purpose indicated by the manufacturer in the instructions for use, promotional or sales materials and statements, or technical documentation, but that may result from reasonably foreseeable human behaviour or technical operation or interaction. | **F** | |
| **A3, point 25** | (25) 'reasonably foreseeable misuse' means the use of a product with digital elements in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems; | | **A3, point 25** | 25. "Reasonably foreseeable misuse" means the use of a product with digital elements in a way that is not in accordance with its intended purpose, but that may result from reasonably foreseeable human behaviour or interaction with other systems. | **F** | |
| **A3, point 26** | (26) 'notifying authority' means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, | | **A3, point 26** | 26. "Notifying authority" means the national authority responsible for establishing and carrying out the procedures necessary for the assessment, designation and notification of | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | designation and notification of conformity assessment bodies and for their monitoring; | | | conformity assessment bodies and for monitoring them. | | |
| **A3, point 27** | (27) 'conformity assessment' means the process of verifying whether the essential cybersecurity requirements set out in Annex I have been fulfilled; | | **A3, point 27** | 27. "Conformity assessment" means the process of verifying whether the essential cybersecurity requirements set out in annex I to this law have been fulfilled. | **F** | |
| **A3, point 28** | (28) 'conformity assessment body' means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008; | | **A3, point 28** | 28. "Conformity assessment body" has the same meaning as under law No. 116/2014 "On the Accreditation of Conformity Assessment Bodies in the Republic of Albania", as amended. | **F** | |
| **A3, point 29** | (29) 'notified body' means a conformity assessment body designated in accordance with Article 43 and other relevant Union harmonisation legislation; | | **A3, point 29** | 29. "Notified body" means a conformity assessment body designated in accordance with article 43 of this law and the relevant harmonised legislation of the Republic of Albania in force. | **F** | |
| **A3, point 30** | (30) '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 cybersecurity requirements set out in Part I of Annex I or which results in a modification to the intended purpose for which the product with digital elements has been assessed; | | **A3, point 30** | 30. "Substantial modification" means a change to a product with digital elements after it has been placed on the market that affects the product's compliance with the essential cybersecurity requirements set out in part I of annex I to this law, or results in a change to the intended purpose for which the product with digital elements has been assessed. | **F** | |
| **A3, point 31** | (31) '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 cybersecurity requirements set out in Annex I and other applicable Union harmonisation legislation providing for its affixing; | | **A3, point 31** | 31. "CE marking" means a marking by which the manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in annex I to this law and with other relevant legislation in force providing for the affixing of that marking. | **F** | |
| **A3, point 32** | (32) '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; | | **A3, point 32** | 32. "Harmonised legislation" means European Union legislation on market surveillance and product compliance and any other legislation relating to the marketing of products to which that legislation applies. | **P** | |
| **A3, point 33** | (33) 'market surveillance authority' means a market surveillance authority as defined in Article 3, point (4), of Regulation (EU) 2019/1020; | | **A3, point 33** | 33. "Market surveillance responsible structure" means the authority responsible for market surveillance as specified in the legislation in force on market surveillance. | **F** | |
| **A3, point 34** | (34) 'international standard' means an international standard as defined in Article 2, point (1)(a), of Regulation (EU) No 1025/2012; | | **A3, point 34** | 34. "International standard" has the same meaning as in law No. 9870/2008 "On Standardisation", as amended. | **F** | |
| **A3, point 35** | (35) 'European standard' means a European standard as defined in Article 2, point (1)(b), of Regulation (EU) No 1025/2012; | | **A3, point 35** | 35. "European standard" has the same meaning as in law No. 9870/2008 "On Standardisation", as amended. | **F** | |
| **A3, point 36** | (36) 'harmonised standard' means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012; | | **A3, point 36** | 36. "Harmonised standard" has the same meaning as in law No. 9870/2008 "On Standardisation", as amended. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A3, point 37** | (37) 'cybersecurity risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident; | | **A3, point 37** | 37. "Cybersecurity risk" has the same meaning as in law No. 25/2024 "On Cybersecurity". | | |
| **A3, point 38** | (38) '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; | | **A3, point 38** | 38. "Significant cybersecurity risk" means a cybersecurity risk which, on the basis of its technical characteristics, may be assumed to have a high probability of an incident that could lead to a serious negative impact, including by causing considerable material or non-material loss or disruption. | **F** | |
| **A3, point 39** | (39) '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; | | **A3, point 39** | 39. "Software bill of materials" means a formal record containing details of and supply-chain relationships between the components included in the software elements of a product with digital elements. | **F** | |
| **A3, point 40** | (40) 'vulnerability' means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat; | | **A3, point 40** | 40. "Vulnerability" has the same meaning as in law No. 25/2024 "On Cybersecurity". | **F** | |
| **A3, point 41** | (41) 'exploitable vulnerability' means a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions; | | **A3, point 41** | 41. "Exploitable vulnerability" means a vulnerability that has the potential to be effectively used by a malicious actor under practical operational conditions. | **F** | |
| **A3, point 42** | (42) 'actively exploited vulnerability' means a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner; | | **A3, point 42** | 42. "Actively exploited vulnerability" means a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without the permission of the system owner. | **F** | |
| **A3, point 43** | (43) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555; | | **A3, point 43** | 43. "Incident" has the same meaning as in law No. 25/2024 "On Cybersecurity". | **F** | |
| **A3, point 44** | (44) 'incident having an impact on the security of the product with digital elements' means an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions; | | **A3, point 44** | 44. "Incident having an impact on the security of a product with digital elements" means an incident that negatively affects, or is capable of negatively affecting, the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions. | **F** | |
| **A3, point 45** | (45) 'near miss' means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555; | | **A3, point 45** | 45. "Near miss" means an event that could have compromised the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or of services offered by, or accessible via, network and information systems, but was successfully prevented from materialising or did not materialise. | **F** | |
| **A3, point 46** | (46) 'cyber threat' means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881; | | **A3, point 46** | 46. "Cyber threat" has the same meaning as in law No. 25/2024 "On Cybersecurity" | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A3, point 47** | (47) 'personal data' means personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679; | | **A3, point 47** | 47. "Personal data" has the same meaning as in law No. 124/2024 "On the Protection of Personal Data". | **F** | |
| **A3, point 48** | (48) 'free and open-source software' means software the source code of which is openly shared and which is made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable; | | **A3, point 48** | 48. "Free and open-source software" means software whose source code is openly shared and which is made available under a free and open-source licence that provides all rights to make it freely accessible, usable, modifiable and redistributable. | **F** | |
| **A3, point 49** | (49) 'recall' means recall as defined in Article 3, point (22), of Regulation (EU) 2019/1020; | | **A3, point 49** | 49. "Recall" means any measure aimed at achieving the return of a product that has already been made available to the end user. | **F** | |
| **A3, point 50** | (50) 'withdrawal' means withdrawal as defined in Article 3, point (23), of Regulation (EU) 2019/1020; | | **A3, point 50** | 50. "Withdrawal" means any measure aimed at preventing a product in the supply chain from being made available on the market. | **F** | |
| **A3, point 51** | (51) 'CSIRT designated as coordinator' means a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555. | | **A3, point 51** | 51. "CSIRT designated as coordinator" means the National CSIRT under law No. 25/2024 "On Cybersecurity". | **F** | |
| **A4** | Article 4<br>**Free movement**<br><br>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.<br>2. At trade fairs, exhibitions, demonstrations or similar events, Member States shall not prevent the presentation or use of a product with digital elements which does not comply with this Regulation, including its prototypes, provided that the product is presented with a visible sign clearly indicating that it does not comply with this Regulation and that it is not to be made available on the market until it does so.<br>3. Member States shall not prevent the making available on the market of unfinished software which does not comply with this Regulation, provided that the software is made available only for a limited period required for testing purposes with a visible sign clearly indicating that it does not comply with this Regulation and that it will not be available on the market for purposes other than testing.<br>4. Paragraph 3 does not apply to safety components as referred to in Union harmonisation legislation other than this Regulation. | | **A4** | Article 4<br>**Free movement**<br><br>1. Products with digital elements shall be made available on the market and put into service only if they comply with the requirements of this law.<br>2. At trade fairs, exhibitions, demonstrations or similar events, the presentation or use of a product with digital elements that does not comply with this law, including a prototype, shall not be prevented, provided that the product is accompanied by a visible sign clearly indicating that it does not comply with this law and that the product with digital elements shall not be made available on the market until it complies with the relevant requirements.<br>3. The making available on the market of unfinished software that does not comply with this law shall not be prevented, provided that the software is made available only for a limited period required for testing purposes and is accompanied by a visible sign clearly indicating that it does not comply with this law and shall not be made available on the market for any purpose other than testing. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | 4. Point 3 of this article shall not apply to safety components provided for in national legislation other than this law. | | |
| **A5** | Article 5<br>**Procurement or use of products with digital elements**<br><br>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, including where those products are procured or used for national security or defence purposes, provided that such requirements are consistent with Member States' obligations laid down in Union law and that they are necessary and proportionate for the achievement of those purposes.<br>2. Without prejudice to Directives 2014/24/EU and 2014/25/EU, where products with digital elements that fall within the scope of this Regulation are procured, Member States shall ensure that compliance with the essential cybersecurity requirements set out in Annex I to this Regulation, including the manufacturers' ability to handle vulnerabilities effectively, are taken into consideration in the procurement process. | | **A5** | Article 5<br>**Procurement or use of products with digital elements**<br><br>1. Public authorities may lay down additional cybersecurity requirements for the procurement or use of products with digital elements for specific purposes, including where such products are procured or used for national security or defence purposes, provided that those requirements comply with the obligations arising from the relevant legislation and are necessary and proportionate to achieve those purposes.<br>2. Without prejudice to public procurement legislation, when procuring products with digital elements falling within the scope of this law, public authorities shall ensure that compliance with the essential cybersecurity requirements set out in annex I to this law is taken into account, including the manufacturers" ability to handle vulnerabilities effectively. | **F** | |
| **A6** | Article 6<br>**Requirements for products with digital elements**<br><br>Products with digital elements shall be made available on the market only where:<br><br>(a) they meet the essential cybersecurity requirements set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed; and<br>(b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I. | | **A6** | Article 6<br>**Requirements for products with digital elements**<br><br>Products with digital elements shall be made available on the market only where:<br>a. they meet the essential cybersecurity requirements set out in part I of annex I to this law, provided that they are properly installed, maintained and used for their intended purpose or under reasonably foreseeable conditions and, where applicable, the necessary security updates have been installed; and<br>b. the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in part II of annex I to this law. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A7** | Article 7<br>**Important products with digital elements**<br><br>1. Products with digital elements which have the core functionality of a product category set out in Annex III shall be considered to be important products with digital elements and shall be subject to the conformity assessment procedures referred to in Article 32(2) and (3). The integration of a product with digital elements which has the core functionality of a product category set out in Annex III shall not in itself render the product in which it is integrated subject to the conformity assessment procedures referred to in Article 32(2) and (3).<br>2. The categories of products with digital elements referred to in paragraph 1 of this Article, divided into classes I and II as set out in Annex III, meet at least one of the following criteria:<br>(a) the product with digital elements primarily performs functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, end-point security or network protection;<br>(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, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.<br>3. The Commission is empowered to adopt delegated acts in accordance with Article 61 to amend Annex III by including in the list a new category within each class of the categories of products with digital elements and specifying its definition, moving a category of products from one class to the other or withdrawing an existing category from that list. When assessing the need to amend the list set out in Annex III, the Commission shall take into account the 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 referred to in paragraph 2 of this Article.<br>The delegated acts referred to in the first subparagraph of this paragraph shall, where appropriate, provide for a minimum transitional period of 12 months, in particular where a new category of important products with digital elements is added to class I or II or is moved from class I to II as set out in Annex III, before the relevant | | **A7** | Article 7<br>**Important products with digital elements**<br><br>1. Products with digital elements that have the core functionality of a product category listed in annex III to this law shall be considered important products with digital elements and shall be subject to the conformity assessment procedures set out in points 2 and 3 of article 32 of this law. The integration of a product with digital elements that has the core functionality of a product category listed in Annex III to this law shall not make the product into which it is integrated subject to the conformity assessment procedures referred to in points 2 and 3 of article 32 of this law.<br>2. The categories of products with digital elements referred to in point 1 of this article, divided into Classes I and II in accordance with annex III to this law, shall meet at least one of the following criteria:<br>a. the product with digital elements performs primarily functions that are critical to the cybersecurity of other products, networks or services, including the provision of authentication and access, prevention and detection of intrusions, endpoint security or network protection;<br>b. the product with digital elements performs a function that 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 or safety of users, through direct manipulation, such as a core system function including network management, configuration control, virtualisation or the processing of personal data.<br>3. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall initiate amendments to annex III to this law by adding to the list a new category in each class of products with digital elements and specifying its definition, moving a product category from one class to another, or removing an existing category from that list. When assessing the need for such amendments, the cybersecurity-related functionalities or function, and the level of cybersecurity risk posed by those products, in accordance with the criteria set out in point 2 of this article shall be taken into account.<br>4. Where necessary, on a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall, in | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | conformity assessment procedures as referred to in Article 32(2) and (3) start applying, unless a shorter transitional period is justified on imperative grounds of urgency.<br>4. By 11 December 2025, the Commission shall adopt an implementing act specifying the technical description of the categories of products with digital elements under classes I and II as set out in Annex III and the technical description of the categories of products with digital elements as set out in Annex IV. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 62(2). | | | accordance with point 3 of this article, approve a minimum transitional period of 12 months, in particular where a new category of important products with digital elements is added to class I or II, or moved from class I to class II, in annex III to this law, before the relevant conformity assessment procedures referred to in point 2 and 3 of article 32 of this law start to apply, unless a shorter period is justified by urgency.<br>5. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall approve technical descriptions of the categories of products with digital elements covered by classes I and II set out in annex III to this law, as well as technical descriptions of the categories of products with digital elements set out in annex IV to this law. | | |
| **A8** | Article 8<br>**Critical products with digital elements**<br><br>1. The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation to determine which products with digital elements that have the core functionality of a product category that is set out in Annex IV to this Regulation are to be required to obtain a European cybersecurity certificate at assurance level at least 'substantial' under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881, to demonstrate conformity with the essential cybersecurity requirements set out in Annex I to 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. Those 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 the critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555. Before adopting such delegated acts, the Commission shall carry out an assessment of the potential market impact of the envisaged measures and shall carry out consultations with relevant stakeholders, including the European Cybersecurity Certification Group established under Regulation (EU) 2019/881. The assessment shall take into account the readiness and the capacity level of | | **A8** | Article 8<br>**Critical products with digital elements**<br><br>1. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall determine which products with digital elements having the core functionality of a product category listed in annex IV to this law are required to obtain a cybersecurity certificate at an assurance level of at least "substantial" under a national cybersecurity certification scheme or a European cybersecurity certification scheme, in order to demonstrate conformity with the essential cybersecurity requirements set out in annex I to this law, or parts thereof, provided that a certification scheme covering that category of products with digital elements has been adopted and is available to manufacturers.<br>The required assurance level 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 the critical dependence of critical entities as provided for in annex I to law No. 25/2024 "On Cybersecurity".<br>Before the decision is adopted, an assessment of its potential impact on the market shall be carried out and consultations shall be held with interested parties, including the relevant cybersecurity certification bodies. The assessment shall take account of the readiness and capacity of the | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | the Member States for the implementation of the relevant European cybersecurity certification scheme. Where no delegated acts as referred to in the first subparagraph of this paragraph have been adopted, products with digital elements which have the core functionality of a product category as set out in Annex IV shall be subject to the conformity assessment procedures referred to in Article 32(3).<br>The delegated acts referred to in the first subparagraph shall provide for a minimum transitional period of six months, unless a shorter transitional period is justified for imperative reasons of urgency.<br>2. The Commission is empowered to adopt delegated acts in accordance with Article 61 to amend Annex IV by adding or withdrawing categories of critical products with digital elements. When determining such categories of critical products with digital elements and the required assurance level, in accordance with paragraph 1 of this Article, the Commission shall take into account the criteria referred to in Article 7(2) and ensure that the categories of products with digital elements meet at least one of the following criteria:<br>(a) there is a critical dependency of essential entities as referred to in Article 3 of Directive (EU) 2022/2555 on the category of products with digital elements;<br>(b) incidents and exploited vulnerabilities concerning the category of products with digital elements could lead to serious disruptions of critical supply chains across the internal market.<br>Before adopting such delegated acts, the Commission shall carry out an assessment of the type referred to in paragraph 1.<br>The delegated acts referred to in the first subparagraph shall provide for a minimum transitional period of six months, unless a shorter transitional period is justified for imperative reasons of urgency. | | | authorities and the market to implement the relevant certification scheme.<br>2. Where the decision referred to in point 1 of this article has not been adopted, products with digital elements having the core functionality of a product category listed in annex IV to this law shall be subject to the conformity assessment procedure set out in point 3 of article 32 of this law.<br>3. The decision of the Council of Ministers referred to in point 1 of this article shall provide for a minimum transitional period of six months, unless a shorter transitional period is justified for reasons of imperative urgency.<br>4. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall initiate amendments to annex IV to this law by adding or removing categories of critical products with digital elements in accordance with relevant European Union practice.<br>When determining such categories of critical products with digital elements and the required assurance level in accordance with point 1 of this article, the criteria set out in point 2 of Article 7 of this law shall be taken into account and shall ensure that the categories of products with digital elements meet at least one of the following criteria:<br>a. there is a critical dependence of critical entities, as provided for in annex I to law no. 25/2024 "On Cybersecurity", on the category of products with digital elements;<br>b. incidents or exploited vulnerabilities relating to those categories of products with digital elements could lead to serious disruptions to critical supply chains on the market.<br>5. Before the secondary legislation referred to in this article is adopted, an assessment of the kind referred to in point 1 of this article shall be carried out. The act referred to in point 1 of this article shall provide for a minimum transitional period of six months, unless a shorter period is justified for reasons of imperative urgency. | | |
| **A9** | Article 9<br>**Stakeholder consultation**<br><br>1. When preparing measures for the implementation of this Regulation, the Commission shall consult and take into account the views of relevant stakeholders, such as relevant Member State authorities, private sector undertakings, including microenterprises and small and medium-sized enterprises, the open- | | **A9** | Article 9<br>**Consultation of interested parties**<br><br>1. When preparing measures for the implementation of this law, the competent authorities shall consult and take into account the views of interested parties, including the relevant public authorities, private-sector undertakings, including microenterprises and small and medium- | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | source software community, consumer associations, academia, and relevant Union agencies and bodies as well as expert groups established at Union level. In particular, the Commission shall, in a structured manner, where appropriate, consult and seek the views of those stakeholders when:<br>(a) preparing the guidance referred to in Article 26;<br>(b) preparing the technical descriptions of the product categories set out in Annex III in accordance with Article 7(4), assessing the need for potential updates of the list of product categories in accordance with Article 7(3) and Article 8(2), or carrying out the assessment of the potential market impact referred to in Article 8(1), without prejudice to Article 61;<br>(c) undertaking preparatory work for the evaluation and review of this Regulation.<br>2. The Commission shall organise regular consultation and information sessions, at least once a year, to gather the views of the stakeholders referred to in paragraph 1 on the implementation of this Regulation. | | | sized enterprises, the open-source software community, consumer associations and the academic community. In particular, structured consultation shall be carried out, where appropriate, in the following cases:<br>a. when preparing the guidance referred to in article 26 of this law;<br>b. when preparing the technical descriptions of the product categories set out in annex III to this law, in accordance with point 4 of article 7 of this law, assessing the need for possible updates to the list of product categories in accordance with point 3 of article 7 and point 2 of article 8 of this law, or carrying out the assessment of the potential impact on the market referred to in point 1 of article 8 of this law;<br>c. when carrying out preparatory work for the assessment and review of this law.<br>2. The competent authorities shall organise regular consultation and information meetings, at least once a year, in order to gather the views of the interested parties referred to in point 1 of this article on the implementation of this law. | | |
| **A10** | Article 10<br>**Enhancing skills in a cyber resilient digital environment**<br><br>For the purposes of this Regulation and in order to respond to the needs of professionals in support of the implementation of this Regulation, Member States with, where appropriate, the support of the Commission, the European Cybersecurity Competence Centre and ENISA, while fully respecting the responsibility of the Member States in the education field, shall promote measures and strategies aiming to:<br>(a) develop cybersecurity skills and create organisational and technological tools to ensure sufficient availability of skilled professionals in order to support the activities of the market surveillance authorities and conformity assessment bodies;<br>(b) increase collaboration between the private sector, economic operators, including via re-skilling or up-skilling for manufacturers' employees, consumers, training providers as well as public administrations, thereby expanding the options for young people to access jobs in the cybersecurity sector. | | **A10** | Article 10<br>**Enhancing skills in a cyber digital environment**<br><br>For the purposes of this law and in response to the needs of professionals supporting its implementation, the ministry responsible for the economy, market surveillance, accreditation and vocational training, the ministry responsible for education, the ministry responsible for public administration, the ministry responsible for electronic and digital communications, and the National Cyber Security Authority, in cooperation with the relevant institutions, shall promote measures and strategies aimed at:<br>a. developing cybersecurity skills and establishing organisational and technological tools to ensure an adequate availability of qualified professionals to support the activities of market surveillance authorities and conformity assessment bodies;<br>b. strengthening cooperation between the private sector and economic operators, including the reskilling and upskilling of employees of manufacturers, consumers, training providers and public administration, as well as expanding opportunities for young people to find employment in the cybersecurity sector. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A11** | Article 11<br>**General product safety**<br><br>By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation (EU) 2023/988, Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of that Regulation shall apply to products with digital elements with respect to aspects and risks or categories of risks that are not covered by this Regulation where those products are not subject to specific safety requirements laid down in other 'Union harmonisation legislation' as defined in Article 3, point (27), of Regulation (EU) 2023/988. | | **A11** | Article 11<br>**General product safety**<br><br>Without prejudice to the relevant provisions of the legislation in force on general product safety, the general requirements and principles of that legislation shall apply to products with digital elements in relation to risks or categories of risks not covered by this law, where those products are not subject to specific safety requirements laid down in specific harmonised legislation in accordance with European Union practice. | **F** | |
| **A12** | Article 12<br>**High-risk AI systems**<br><br>1. Without prejudice to the requirements relating to accuracy and robustness set out in Article 15 of Regulation (EU) 2024/1689, products with digital elements which fall within the scope of this Regulation and which are classified as high-risk AI systems pursuant to Article 6 of that Regulation shall be deemed to comply with the cybersecurity requirements set out in Article 15 of that Regulation where:<br>(a) those products fulfil the essential cybersecurity requirements set out in Part I of Annex I;<br>(b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I; and<br>(c) the achievement of the level of cybersecurity protection required under Article 15 of Regulation (EU) 2024/1689 is demonstrated in the EU declaration of conformity issued under this Regulation.<br>2. For the products with digital elements and cybersecurity requirements referred to in paragraph 1 of this Article, the relevant conformity assessment procedure provided for in Article 43 of Regulation (EU) 2024/1689 shall apply. For the purposes of that assessment, notified bodies which are competent to control the conformity of the high-risk AI systems under Regulation (EU) 2024/1689 shall also be competent to control the conformity of 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 39 of this Regulation has been assessed in the context of the notification procedure under Regulation (EU) 2024/1689. | | **A12** | Article 12<br>**High-risk AI systems**<br><br>1. Without prejudice to the requirements relating to accuracy and robustness laid down in the relevant provisions of the legislation in force on artificial intelligence, products with digital elements falling within the scope of this law and classified as high-risk AI systems in accordance with the relevant provisions of the legislation in force on artificial intelligence shall be deemed to comply with the cybersecurity requirements set out in the relevant provisions of the legislation in force on artificial intelligence where:<br>a. they meet the essential cybersecurity requirements set out in part I of annex I to this law;<br>b. the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in part II of annex I to this law; and<br>c. achievement of the cybersecurity protection level required under the relevant provisions of the legislation in force on artificial intelligence is demonstrated in the EU declaration of conformity issued in accordance with this law.<br>2. The relevant conformity assessment procedure provided for in the relevant provisions of the legislation in force on artificial intelligence shall apply to the products with digital elements referred to in point 1 of this article. For the purposes of that assessment, notified bodies competent to assess the conformity of high-risk AI systems under the legislation in force on artificial intelligence shall also be competent to assess the conformity of those systems with the requirements of this law, provided that their compliance with the requirements of article 39 of this law has been verified as part of the | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 3. By way of derogation from paragraph 2 of this Article, important products with digital elements as listed in Annex III to this Regulation, which are subject to the conformity assessment procedures referred to in Article 32(2), points (a) and (b), and Article 32(3) of this Regulation and critical products with digital elements as listed in Annex IV to this Regulation which are required to obtain a European cybersecurity certificate pursuant to Article 8(1) of this Regulation or, absent that, which are subject to the conformity assessment procedures referred to in Article 32(3) of this Regulation, and which are classified as high-risk AI systems pursuant to Article 6 of Regulation (EU) 2024/1689, and to which the conformity assessment procedure based on internal control as referred to in Annex VI to Regulation (EU) 2024/1689 applies, shall be subject to the conformity assessment procedures provided for in this Regulation in so far as the essential cybersecurity requirements set out in this Regulation are concerned.<br>4. Manufacturers of products with digital elements as referred to in paragraph 1 of this Article may participate in the AI regulatory sandboxes referred to in Article 57 of Regulation (EU) 2024/1689. | | | notification procedure under the legislation in force on artificial intelligence.<br>3. By way of derogation from point 2, important products with digital elements listed in annex III to this law that are subject to the conformity assessment procedures provided for in letters a) and b) of point 2 of article 32 and point 3 of article 32 of this law, and critical products with digital elements listed in annex IV to this law that are required to obtain a European cybersecurity certificate in accordance with point 1 of article 8 of this law or, in the absence of such a certificate, are subject to the conformity assessment procedures under point 3 of article 32 of this law, and that are classified as high-risk AI systems under the relevant provisions of the legislation in force on artificial intelligence, shall be subject to the conformity assessment procedures provided for in this law as regards the essential cybersecurity requirements.<br>4. Manufacturers of the products with digital elements referred to in point 1 of this article may participate in regulatory sandboxes for artificial intelligence established under Albanian legislation on artificial intelligence. Participation in a sandbox shall not exempt them from complying with the cybersecurity requirements of this law or from following the conformity assessment procedures. | | |
| **A13** | Article 13<br>**Obligations of manufacturers**<br><br>1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.<br>2. For the purpose of complying with 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 incidents and minimising their impact, including in relation to the health and safety of users.<br>3. The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 | | **A13** | Article 13<br>**Obligations of manufacturers**<br><br>1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in part I of annex I to this law.<br>2. For the purposes of complying with point 1 of this article, manufacturers shall carry out an assessment of the cybersecurity risks associated with a product with digital elements and shall take the results of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product, with the aim of minimising cybersecurity risks, preventing incidents and minimising their impact, including on the health and safety of users.<br>3. The cybersecurity risk assessment shall be documented and updated as necessary during the support period determined in accordance with point 8 | **F** | Point 25 of Article 13 of the regulation relates to member states and is not applicable to the case of Albania. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | of this Article. That cybersecurity risk assessment shall 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 length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.<br>4. When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment referred to in paragraph 3 of this Article in the technical documentation required pursuant to Article 31 and Annex VII. For products with digital elements as referred to in Article 12, which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.<br>5. For the purpose of complying with paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product with digital elements, 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.<br>6. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex I. 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 | | | of this article. That assessment shall include at least an analysis of the 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 expected period of use of the product. The cybersecurity risk assessment shall indicate whether the security requirements set out in annex I, part I, point 2, to this law are applicable to the relevant product with digital elements and how they are applied on the basis of the cybersecurity risk assessment. The assessment shall also indicate how the manufacturer is to apply annex I, part I, point 1, to this law and the vulnerability-handling requirements set out in part II of annex I to this law.<br>4. When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment referred to in point 3 of this article in the technical documentation required under article 31 and annex VII to this law. For products with digital elements referred to in article 12 of this law that are also subject to other legal acts in force, the cybersecurity risk assessment may form part of the risk assessment required by those legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in the technical documentation.<br>5. For the purposes of complying with point 1 of this article, manufacturers shall exercise due diligence when integrating third-party components so that those components do not compromise the cybersecurity of the product with digital elements, including when integrating free and open-source software components that have not been made available on the market in the course of a commercial activity.<br>6. After identifying a vulnerability in a component, including an open-source component, integrated into a product with digital elements, manufacturers shall report that vulnerability to the person or entity manufacturing or maintaining the component, and shall address and remediate the vulnerability in accordance with the vulnerability-handling requirements set out in part II of annex I to this law. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | or maintaining the component, where appropriate in a machine-readable format.<br>7. The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products.<br>8. Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I.<br>Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements. When determining the support period, manufacturers may also take into account the support periods of products with digital elements offering a similar functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components that provide core functions and are sourced from third parties as well as relevant guidance provided by the dedicated administrative cooperation group (ADCO) established pursuant to Article 52(15) and the Commission. The matters to be taken into account in order to determine the support period shall be considered in a manner that ensures proportionality.<br>Without prejudice to the second subparagraph, the support period shall be at least five years. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.<br>Taking into account ADCO recommendations as referred to in Article 52(16), the Commission may adopt delegated acts in accordance with Article 61 to supplement this Regulation by specifying the minimum support period for specific product categories where the market surveillance data suggests inadequate support periods.<br>Manufacturers shall include the information that was taken into account to determine the support period of a | | | relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.<br>7. Manufacturers shall systematically document, in a manner proportionate to the nature and cybersecurity risks, relevant cybersecurity aspects relating to products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products.<br>8. When placing a product with digital elements on the market and throughout the support period, manufacturers shall ensure that vulnerabilities in that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in part II of annex I to this law.<br>Manufacturers shall determine the support period so that it reflects the period during which the product is expected to be in use, taking into account, in particular, the reasonable expectations of users, the nature of the product, including its intended purpose, and the relevant legislation in force that determines the lifetime of products with digital elements. When determining the support period, manufacturers may also take into account the support periods of products with digital elements offering equivalent functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components providing core functionality sourced from third parties, and relevant guidance issued by the dedicated Administrative Cooperation Group (AdCo) established by the European Commission. The factors to be taken into account when determining the support period shall be considered in a manner that ensures proportionality.<br>Without prejudice to the first subpoint, the support period shall be at least five years. Where a product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected period of use.<br>By decision of the Council of Ministers, minimum support periods shall be approved for specific product categories where market surveillance data suggest that support periods are insufficient, in accordance with relevant European Union practice.<br>Manufacturers shall include the information taken into account when determining the support period of | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | product with digital elements in the technical documentation as set out in Annex VII.<br>Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Part II, point (5), of Annex I to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.<br>9. Manufacturers shall ensure that each security update, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer.<br>10. Where a manufacturer has placed subsequent substantially modified versions of a software product on the market, that manufacturer may ensure compliance with the essential cybersecurity requirement set out in Part II, point (2), of Annex I only for the version that it has last placed on the market, provided that the users of the versions that were previously placed on the market have access to the version last placed on the market free of charge and do not incur additional costs to adjust the hardware and software environment in which they use the original version of that product.<br>11. Manufacturers may maintain public software archives enhancing user access to historical versions. In those cases, users shall be clearly informed in an easily accessible manner about risks associated with using unsupported software.<br>12. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 31.<br>They shall carry out the chosen conformity assessment procedures as referred to in Article 32 or have them carried out.<br>Where compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 28 and affix the CE marking in accordance with Article 30.<br>13. Manufacturers shall keep the technical documentation and the EU declaration of conformity at the disposal of the market surveillance authorities for at least 10 years after the product with digital elements has | | | a product with digital elements in the technical documentation referred to in annex VII to this law.<br>Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies as referred to in annex I, part II, point 5, to this law, for processing and remediating potential vulnerabilities in the product with digital elements reported from internal or external sources.<br>9. Manufacturers shall ensure that every security update referred to in annex I, Part II, point 8, to this law, which is made available to users during the support period, remains available after its release for at least 10 years or for the remainder of the support period, whichever is longer.<br>10. Where a manufacturer has placed on the market subsequent substantially modified versions of a software product, that manufacturer may ensure compliance with the essential cybersecurity requirement set out in annex I, part II, point 2, to this law only for the version most recently placed on the market, provided that users of versions previously placed on the market have access to the latest version free of charge and do not incur additional costs to adapt the hardware or software environment in which they use the original version of that product.<br>11. Manufacturers may maintain public software archives, thereby increasing users' access to historical versions. In such cases, users shall be clearly informed, in an easily accessible manner, of the risks associated with using unsupported software.<br>12. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation in accordance with article 31 of this law.<br>They shall carry out the conformity assessment procedures they have selected, as referred to in article 32 of this law, or ensure that those procedures are carried out.<br>Where that conformity assessment procedure has demonstrated that the product with digital elements complies with the essential cybersecurity requirements set out in part I of annex I to this law and that the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in part II of annex I to this law, manufacturers shall draw up the EU declaration of conformity in accordance with article 28 of this law and affix the CE marking in accordance with article 30 of this law. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | been placed on the market or for the support period, whichever is longer.<br>14. 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 this Regulation. Manufacturers 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 common specifications as referred to in Article 27 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.<br>15. 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, that that information is provided on their packaging or in a document accompanying the product with digital elements.<br>16. Manufacturers shall indicate the name, registered trade name or registered trademark of the manufacturer, and the postal address, email address or other digital contact details, as well as, where applicable, the website where the manufacturer can be contacted, on the product with digital elements, on its packaging or in a document accompanying the product with digital elements. That information shall also be included in the information and instructions to the user set out in Annex II. The contact details shall be in a language which can be easily understood by users and market surveillance authorities.<br>17. For the purposes of this Regulation, manufacturers shall designate a single point of contact to enable users to communicate directly and rapidly with them, including in order to facilitate reporting on vulnerabilities of the product with digital elements.<br>Manufacturers shall ensure that the single point of contact is easily identifiable by the users. They shall also include the single point of contact in the information and instructions to the user set out in Annex II.<br>The single point of contact shall allow users to choose their preferred means of communication and shall not limit such means to automated tools.<br>18. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions to the user set out in Annex II, in paper or electronic form. Such information and instructions shall be provided in a language which can | | | 13. Manufacturers shall keep the technical documentation and the EU declaration of conformity available to the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.<br>14. Manufacturers shall ensure that procedures are in place to ensure that products with digital elements that are part of a production series remain in conformity with this law. Manufacturers shall take due account of changes to the development and production process or to the design or characteristics of the product with digital elements, and of changes to the harmonised standards, national or European cybersecurity certification schemes, or common specifications referred to in article 27 of this law, by reference to which conformity of the product with digital elements is declared or through the application of which its conformity is verified.<br>15. Manufacturers shall ensure that their products with digital elements bear a type, batch or serial number or another element allowing their identification or, where that is not possible, that the required information is provided on the packaging or in a document accompanying the product with digital elements.<br>16. Manufacturers shall indicate the manufacturer's name, registered trade name or registered trademark and postal address, email address or other digital contact details, and, where applicable, the website through which the manufacturer can be contacted, on the product with digital elements, its packaging or a document accompanying the product. This information shall also be included in the user information and instructions referred to in annex II to this law. The contact details shall be provided in a language that can be easily understood by users and the market surveillance authorities.<br>17. For the purposes of this law, manufacturers shall designate a single point of contact through which users can communicate directly and rapidly with them, including to facilitate the reporting of vulnerabilities in the product with digital elements.<br>Manufacturers shall ensure that the single point of contact is easily identifiable by users and is included in the user information and instructions referred to in annex II to this law.<br>The single point of contact shall enable users to choose their preferred means of communication and shall not limit those means to automated tools. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | be easily understood by users and market surveillance authorities. They shall be clear, understandable, intelligible and legible. They shall allow for the secure installation, operation and use of products with digital elements. Manufacturers shall keep the information and instructions to the user set out in Annex II at the disposal of users and market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. Where such information and instructions are provided online, manufacturers shall ensure that they are accessible, user-friendly and available online for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.<br>19. Manufacturers shall ensure that the end date of the support period referred to in paragraph 8, including at least the month and the year, 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.<br>Where technically feasible in light of the nature of the product with digital elements, manufacturers shall display a notification to users informing them that their product with digital elements has reached the end of its support period.<br>20. 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 internet address at which the full EU declaration of conformity can be accessed.<br>21. From the placing on the market and for the support period, 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 cybersecurity requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, or to withdraw or recall the product, as appropriate.<br>22. Manufacturers shall, upon a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by that authority, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product | | | 18. Manufacturers shall ensure that products with digital elements are accompanied by the user information and instructions referred to in annex II to this law, in paper or electronic form. The information and instructions shall be provided in a language that can be easily understood by users and the market surveillance authorities. They shall be clear, understandable and legible, and shall enable the safe installation, operation and use of the products with digital elements. Manufacturers shall keep the user information and instructions referred to in annex II to this law available to users and the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. Where such information and instructions are provided online, manufacturers shall ensure that they remain accessible, easy to use and available online for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.<br>19. Manufacturers shall ensure that the end date of the support period referred to in point 8 of this article, including at least the month and year, is clearly and comprehensibly 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.<br>Where technically feasible for the type of product with digital elements, manufacturers shall display a notification informing users that their product with digital elements has reached the end of its support period.<br>20. Manufacturers shall provide with the product with digital elements a copy of the EU declaration of conformity or a simplified EU declaration of conformity. Where a simplified EU declaration of conformity is provided, it shall contain the exact internet address at which the full EU declaration of conformity can be accessed.<br>21. From the time a product is made available on the market and throughout the support period, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer do not comply with the essential cybersecurity requirements set out in annex I to this law shall immediately take the necessary corrective measures to bring the product or those processes into conformity with this law, or to withdraw or recall the product, as appropriate. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Annex I. Manufacturers shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements which they have placed on the market.<br>23. A manufacturer that ceases its operations and, as a result, is not able to comply with this Regulation shall inform, before the cessation of operations takes effect, the relevant market surveillance authorities as well as, by any means available and to the extent possible, the users of the relevant products with digital elements placed on the market, of the impending cessation of operations.<br>24. The Commission may, by means of implementing acts taking into account European or international standards and best practices, specify the format and elements of the software bill of materials referred to in Part II, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).<br>25. In order to assess the dependence of Member States and of the Union as a whole on software components and in particular on components qualifying as free and open-source software, ADCO may decide to conduct a Union wide dependency assessment for specific categories of products with digital elements. For that purpose, market surveillance authorities may request manufacturers of such categories of products with digital elements to provide the relevant software bills of materials as referred to in Part II, point (1), of Annex I. On the basis of such information, the market surveillance authorities may provide ADCO with anonymised and aggregated information about software dependencies. ADCO shall submit a report on the results of the dependency assessment to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555. | | | 22. At the reasoned request of the market surveillance responsible structure, manufacturers shall provide that authority with all the information and documentation, in paper or electronic form and in a language that can be easily understood, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by the manufacturer with the essential cybersecurity requirements set out in annex I to this law. At the authority's request, manufacturers shall cooperate with the market surveillance responsible structure on any action taken to eliminate the cybersecurity risks posed by a product with digital elements that they have placed on the market.<br>23. A manufacturer that ceases its operations and, as a result, is unable to comply with this law shall, before the cessation takes effect, inform the market surveillance responsible structure s and, by any available means and to the extent possible, users of the relevant products with digital elements placed on the market of the impending cessation of its operations.<br>24. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall approve the formats and elements of the software bill of materials referred to in annex I, part II, point 1, to this law, in accordance with relevant European Union practice. | | |
| **A14** | Article 14<br>**Reporting obligations of manufacturers**<br><br>1. A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16. | | **A14** | Article 14<br>**Reporting obligations of manufacturers**<br><br>1. A manufacturer shall simultaneously notify the National CSIRT, as specified in paragraph 7 of this Article, and, upon accession to the European Union, ENISA, of any actively exploited vulnerability contained in a product with digital elements of which it becomes aware. The manufacturer shall report the actively exploited vulnerability through the single reporting platform referred to in Article | **F** | Points 7, 9, and 10 of Article 14 of the regulation relate to notifications by manufacturers in Member States and are partially applicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 2. For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:<br>(a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;<br>(b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;<br>(c) unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available, including at least the following:<br>(i) a description of the vulnerability, including its severity and impact;<br>(ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;<br>(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.<br>3. A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.<br>4. For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:<br>(a) an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member | | | 16 of this Law, upon accession to the European Union.<br>2. For the purposes of the notification referred to in paragraph 1 of this Article, the manufacturer shall submit:<br>a) an early warning notification of an actively exploited vulnerability, immediately and without undue delay and, in any event, within 24 hours of becoming aware of the vulnerability, indicating, where applicable, upon accession to the EU, the Member States in whose territories the manufacturer is aware that its product with digital elements has been made available;<br>b) where the relevant information has not already been provided, a vulnerability notification, immediately and without undue delay and, in any event, within 72 hours of becoming aware of the actively exploited vulnerability, providing general information, to the extent available, about the product with digital elements concerned, the general nature of the exploitation and the vulnerability in question, as well as any corrective or mitigating measures taken and the corrective or mitigating measures that users may undertake. The notification shall also indicate, where applicable, how sensitive the manufacturer considers the information being reported to be;<br>c) where the relevant information has not already been provided, a final report, no later than 14 days after a corrective or mitigating measure has been made available, including at least the following:<br>i. a description of the vulnerability, including its severity and impact;<br>ii. where available, information relating to any malicious actor that has exploited or is exploiting the vulnerability;<br>iii. details of the security update or other corrective measures made available to remedy the vulnerability.<br>3. A manufacturer shall notify the National CSIRT, in accordance with paragraph 7 of this Article, and, upon accession to the EU, ENISA, simultaneously of any serious incident having an impact on the security of a product with digital elements of which it becomes aware. The manufacturer shall report the incident through the single reporting platform established in accordance with Article 16 of this Law, upon accession to the EU. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | States on the territory of which the manufacturer is aware that their product with digital elements has been made available;<br>(b) unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;<br>(c) unless the relevant information has already been provided, a final report, within one month after the submission of the incident notification under point (b), including at least the following:<br>(i) a detailed description of the incident, including its severity and impact;<br>(ii) the type of threat or root cause that is likely to have triggered the incident;<br>(iii) applied and ongoing mitigation measures.<br><br>5. For the purposes of paragraph 3, an incident having an impact on the security of the product with digital elements shall be considered to be severe where:<br>(a) it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or<br>(b) it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.<br>6. Where necessary, the CSIRT designated as coordinator initially receiving the notification may request manufacturers to provide an intermediate report on relevant status updates about the actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements.<br>7. The notifications referred to in paragraphs 1 and 3 of this Article shall be submitted via the single reporting platform referred to in Article 16 using one of the electronic notification end-points referred to in Article 16(1). The notification shall be submitted using the electronic notification end-point of the CSIRT designated as coordinator of the Member State where the | | | 4. For the purposes of the notification referred to in paragraph 3 of this Article, the manufacturer shall submit:<br>a) an early warning notification of a serious incident having an impact on the security of a product with digital elements, immediately and without undue delay and, in any event, within 24 hours of becoming aware of the incident. The notification shall include at least an indication of whether the incident is suspected to have been caused by unlawful or malicious acts and shall also indicate, where applicable, the Member States in whose territories the manufacturer is aware that its product with digital elements has been made available;<br>b) where the relevant information has not already been provided, an incident notification, immediately and without undue delay and, in any event, within 72 hours of becoming aware of the incident, providing general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken and the corrective or mitigating measures that users may undertake. The notification shall also indicate, where applicable, how sensitive the manufacturer considers the information being reported to be;<br>c) where the relevant information has not already been provided, a final report, within one month of submitting the incident notification referred to in point (b), including at least the following:<br>i. a detailed description of the incident, including its severity and impact;<br>ii. the type of threat or root cause that is likely to have triggered the incident;<br>iii. the mitigating measures implemented and those that are ongoing.<br>5. For the purposes of paragraph 3 of this Article, an incident having an impact on the security of a product with digital elements shall be considered serious where:<br>a) it adversely affects, or is capable of adversely affecting, the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of important or sensitive functions or data; or<br>b) it has led, or is capable of leading, to the introduction or execution of malicious code in a product with digital elements or in the networks and information systems of a user of a product with digital elements. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | manufacturers have their main establishment in the Union and shall be simultaneously accessible to ENISA. 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. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the manufacturer concerned has the establishment with the highest number of employees in the Union.<br>Where a manufacturer has no main establishment in the Union, it shall submit the notifications referred to in paragraphs 1 and 3 using the electronic notification end-point of the CSIRT designated as coordinator in the Member State determined pursuant to the following order and based on the information available to the manufacturer:<br>(a) the Member State in which the authorised representative acting on behalf of the manufacturer for the highest number of products with digital elements of that manufacturer is established;<br>(b) the Member State in which the importer placing on the market the highest number of products with digital elements of that manufacturer is established;<br>(c) the Member State in which the distributor making available on the market the highest number of products with digital elements of that manufacturer is established;<br>(d) the Member State in which the highest number of users of products with digital elements of that manufacturer are located.<br>In relation to the third subparagraph, point (d), a manufacturer may submit notifications related to any subsequent actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements to the same CSIRT designated as coordinator to which it first reported.<br>8. After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with | | | 6. Where necessary, upon receipt of a notification, the National CSIRT may request manufacturers to provide an interim report on relevant status updates concerning the actively exploited vulnerability or the serious incident having an impact on the security of the product with digital elements.<br>7. Upon accession to the EU, the notifications referred to in paragraphs 1 and 3 of this Article shall be submitted through the single reporting platform referred to in Article 16 of this Law.<br>8. Upon becoming aware of an actively exploited vulnerability or a serious incident having an impact on the security of a product with digital elements, the manufacturer shall inform the affected users of the product with digital elements and, where appropriate, all users, of that vulnerability or incident and, where necessary, of any risk-mitigating and corrective measures that users may apply to mitigate the impact of that vulnerability or incident. Where appropriate, such information shall be provided in a structured, electronically readable and easily machine-processable format.<br>Where the manufacturer fails to inform users of the product with digital elements in a timely manner, the National CSIRT may provide such information to users where this is considered proportionate and necessary to prevent or mitigate the impact of the vulnerability or incident.<br>9. The Council of Ministers, upon the proposal of the Minister responsible for electronic and digital communications, shall approve the format and procedures for the notifications referred to in this Article, in accordance with the relevant practices of the European Union. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.<br>9. By 11 December 2025, the Commission shall adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications as referred to in Article 16(2) of this Regulation. The Commission shall cooperate with the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555 and ENISA in preparing the draft delegated acts.<br>10. The Commission may, by means of implementing acts, specify further the format and procedures of the notifications referred to in this Article as well as in Articles 15 and 16. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). The Commission shall cooperate with the CSIRTs network and ENISA in preparing those draft implementing acts. | | | | | |
| **A15** | Article 15<br>**Voluntary reporting**<br><br>1. Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA.<br>2. Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.<br>3. The CSIRT designated as coordinator or ENISA shall process the notifications referred to in paragraphs 1 and 2 of this Article in accordance with the procedure laid down in Article 16.<br>The CSIRT designated as coordinator may prioritise the processing of mandatory notifications over voluntary notifications.<br>4. Where a natural or legal person other than the manufacturer notifies an actively exploited vulnerability or a severe incident having an impact on the security of a product with digital elements in | | | **Article 15**<br>**Voluntary reporting**<br><br>1. Manufacturers, as well as other natural or legal persons, may voluntarily report to the National CSIRT any vulnerability contained in a product with digital elements, as well as cyber threats that may affect the risk profile of a product with digital elements.<br>2. Manufacturers, as well as other natural or legal persons, may voluntarily report to the National CSIRT any incident having an impact on the security of a product with digital elements, as well as near misses.<br>3. Upon accession to the EU, the National CSIRT shall process the notifications referred to in paragraphs 1 and 2 of this Article in accordance with the procedure laid down in Article 16 of this Law.<br>The National CSIRT may give priority to the processing of mandatory notifications over voluntary notifications.<br>4. Where a natural or legal person other than the manufacturer reports an actively exploited vulnerability or a serious incident having an impact on the security of a product with digital elements in accordance with paragraphs 1 or 2 of this Article, | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | accordance with paragraph 1 or 2, the CSIRT designated as coordinator shall without undue delay inform the manufacturer.<br>5. The CSIRTs designated as coordinators as well as ENISA shall ensure the confidentiality and appropriate protection of the information provided by a notifying natural or legal person. 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 a notifying natural or legal person to which it would not have been subject had it not submitted the notification. | | | the National CSIRT shall inform the manufacturer immediately.<br>5. The National CSIRT shall ensure the confidentiality and appropriate protection of the information provided by the reporting natural or legal person. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of additional obligations on the reporting natural or legal person to which that person would not have been subject had they not submitted the notification. | | |
| **A16** | Article 16<br>**Establishment of a single reporting platform**<br><br>1. For the purposes of the notifications referred to in Article 14(1) and (3) and Article 15(1) and (2) and in order to simplify the reporting obligations of manufacturers, a single reporting platform shall be established by ENISA. The day-to-day operations of that single reporting platform shall be 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 end-points.<br>2. After receiving a notification, the CSIRT designated as coordinator initially receiving the notification shall, without delay, disseminate the notification via the single reporting platform to the CSIRTs designated as coordinators on the territory of which the manufacturer has indicated that the product with digital elements has been made available.<br>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 Article 14(2), point (a), of this Regulation, the dissemination of the notification may be delayed based on justified cybersecurity-related grounds for a period of time that is strictly necessary, including where a vulnerability is subject to a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555. Where a CSIRT decides to withhold a notification, it shall immediately inform ENISA about the decision and provide both a justification for withholding the notification as well as an indication of when it will disseminate the notification in accordance with the dissemination procedure laid down in this paragraph. | | | Article 16<br>**Establishment of the single reporting platform**<br><br>1. Upon accession to the European Union, the notifications referred to in paragraphs 1 and 3 of Article 14 and paragraphs 1 and 2 of Article 15 of this Law shall be submitted through the single reporting platform established by ENISA, with a view to simplifying manufacturers' reporting obligations.<br>2. Upon accession to the European Union, following receipt of a notification, the CSIRT designated as coordinator that initially receives the notification shall, without undue delay, disseminate the notification through the single reporting platform to the CSIRTs designated as coordinators in the territories of which the manufacturer has indicated that the product with digital elements has been made available.<br>In exceptional circumstances and, in particular, at the request of the manufacturer, and taking into account the level of sensitivity of the reported information, as indicated by the manufacturer pursuant to point (a) of paragraph 2 of Article 14 of this Law, the dissemination of the notification may be delayed for a period of time necessary on duly justified cybersecurity-related grounds, including where a vulnerability is subject to a coordinated vulnerability disclosure procedure in accordance with the applicable legislation on cybersecurity.<br>Upon accession to the European Union, where the CSIRT decides not to forward a notification, it shall immediately inform ENISA of that decision and provide reasons for not disseminating the notification, together with an indication of when it intends to disseminate the notification in | **F** | Provisions concerning the competencies of ENISA have not been incorporated into Albanian legislation. Consequently, paragraphs 4 and 5 of Article 16 are not applicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | ENISA may support the CSIRT on the application of cybersecurity-related grounds in relation to delaying the dissemination of the notification.<br>In particularly exceptional circumstances, where the manufacturer indicates in the notification referred to in Article 14(2), point (b):<br>(a) that the notified vulnerability has been actively exploited by a malicious actor and, according to the information available, it has been exploited in no other Member State than the one of the CSIRT designated as coordinator to which the manufacturer has notified the vulnerability;<br>(b) that any immediate further dissemination of the notified vulnerability would likely result in the supply of information the disclosure of which would be contrary to the essential interests of that Member State; or<br>(c) that the notified vulnerability poses an imminent high cybersecurity risk stemming from the further dissemination;<br>only the information that a notification was made by the manufacturer, the general information about the product, the information on the general nature of the exploit and the information that security related grounds were raised are to be made available simultaneously to ENISA until the full notification is disseminated to the CSIRTs concerned and ENISA. Where, based on that information, ENISA considers that there is a systemic risk affecting security in the internal market, it shall recommend to the recipient CSIRT that it disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.<br>3. After receiving a notification of an actively exploited vulnerability in a product with digital elements or of a severe incident having an impact on the security of a product with digital elements, the CSIRTs designated as coordinators shall provide the 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.<br>4. ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single reporting platform and the information submitted or disseminated via the single reporting platform. It shall notify without undue delay any security incident affecting the single reporting platform to the CSIRTs network as well as to the Commission. | | | accordance with the procedure laid down in this paragraph.<br>In particularly exceptional circumstances, where the manufacturer indicates in the notification referred to in point (b) of paragraph 2 of Article 14 of this Law that:<br>a) the reported vulnerability has been actively exploited by a malicious actor and, according to the available information, has not been exploited in any other State apart from the State of the CSIRT designated as coordinator to which the manufacturer reported the vulnerability;<br>b) any immediate dissemination of the reported vulnerability is likely to result in the disclosure of information, the disclosure of which would be contrary to the essential interests of that State; or<br>c) the reported vulnerability poses an imminent high cybersecurity risk arising from further dissemination;<br>only the information that a notification has been submitted by the manufacturer, general information about the product, information concerning the general nature of the exploitation, and information indicating that security-related issues have been raised shall be made available to ENISA simultaneously, until the full notification is disseminated to the relevant CSIRTs and ENISA.<br>3. Upon receipt of a notification concerning an actively exploited vulnerability in a product with digital elements or a serious incident having an impact on the security of a product with digital elements, the National CSIRT shall provide the market surveillance responsible structures with the reported information necessary for those structures to fulfil their obligations under this Law.<br>4. Where the National CSIRT becomes aware of an actively exploited vulnerability as part of a coordinated vulnerability disclosure procedure, in accordance with the applicable legislation on cybersecurity, upon accession to the EU, the National CSIRT may, upon receipt of the notification, delay the dissemination of the relevant notification through the single reporting platform on duly justified cybersecurity-related grounds, for a period no longer than necessary and until consent to disclosure has been given by the parties involved in the coordinated vulnerability disclosure procedure.<br>This requirement shall not prevent manufacturers from voluntarily reporting a vulnerability in | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 5. ENISA, in cooperation with the CSIRTs network, shall provide and implement specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single reporting platform referred to in paragraph 1, including at least the security arrangements related to the establishment, operation and maintenance of the single reporting platform, as well as the electronic notification end-points set up by the CSIRTs designated as coordinators at national level and ENISA at Union level, including procedural aspects to ensure that, where a notified vulnerability has no corrective or mitigating measures available, information about that vulnerability is shared in line with strict security protocols and on a need-to-know basis.<br>6. Where a CSIRT designated as coordinator 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 CSIRT designated as coordinator initially receiving the notification may delay the dissemination of the relevant notification via the single reporting platform based on justified cybersecurity-related grounds for a period that is no longer than is strictly necessary and until consent for disclosure by the involved coordinated vulnerability disclosure parties is given. That requirement shall not prevent manufacturers from notifying such a vulnerability on a voluntary basis in accordance with the procedure laid down in this Article. | | | accordance with the procedure laid down in this Article. | | |
| **A17** | Article 17<br>**Other provisions related to reporting**<br><br>1. ENISA may submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established under Article 16 of Directive (EU) 2022/2555 information notified pursuant to Article 14(1) and (3) and Article 15(1) and (2) of this Regulation if such information is relevant for the coordinated management of 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.<br>2. Where public awareness is necessary to prevent or mitigate a severe incident having an impact on the security of the product with digital elements or to handle an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the CSIRT designated as coordinator of the relevant Member State | | | Article 17<br>**Other reporting provisions**<br><br>1. Where public awareness is necessary to prevent or mitigate a severe incident having an impact on the security of a product with digital elements or to address an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the National CSIRT may, after consulting the manufacturer concerned, inform the public about the incident or require the manufacturer to do so.<br>2. On the basis of notifications received in accordance with point 1 and 3 of article 14 and point 1 and 2 of Article 15, of this law, the Authority shall prepare, every 24 months, a technical report on emerging trends in cybersecurity risks relating to products with digital elements and, upon Albania's accession to the European Union, submit it to the European Union Cooperation Group. | **F** | Article 17, paragraph 1 of the regulation concerns reporting between ENISA and EU-CyCLONe and is, as such, inapplicable. Meanwhile, paragraphs 3 and 5 are partially inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | may, after consulting the manufacturer concerned and, where appropriate, in cooperation with ENISA, inform the public about the incident or require the manufacturer to do so.<br>3. ENISA, on the basis of the notifications received pursuant to Article 14(1) and (3) and Article 15(1) and (2) of this Regulation, shall prepare, every 24 months, a technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555. The first such report shall be submitted within 24 months of the date of application of the obligations laid down in Article 14(1) and (3) of this Regulation. 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.<br>4. The mere act of notification in accordance with Article 14(1) and (3) or Article 15(1) and (2) shall not subject the notifying natural or legal person to increased liability.<br>5. After a security update or another form of corrective or mitigating measure is available, ENISA shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified pursuant to Article 14(1) or Article 15(1) of this Regulation to the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555.<br>6. The CSIRTs designated as coordinators shall provide helpdesk support in relation to the reporting obligations pursuant to Article 14 to manufacturers and in particular manufacturers that qualify as microenterprises or as small or medium-sized enterprises. | | | 3. Making a notification in accordance with points 1 and 3 of Article 14 or points 1 and 2 of Article 15 of this law shall not make the notifying natural or legal person subject to increased liability.<br>4. Once a security update or another form of corrective or mitigating measure is available, the Authority shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified in accordance with point 1 of article 14 or point 1 of article 15 of this law to the vulnerability register established in accordance with point 5 of article 14 of law no. 25/2024 “On Cybersecurity”.<br>5. The National CSIRT shall provide support to manufacturers in relation to their reporting obligations under article 14 of this law, in particular to manufacturers that qualify as microenterprises or small and medium-sized enterprises. | | |
| **A18** | Article 18<br>**Authorised representatives**<br><br>1. A manufacturer may, by a written mandate, appoint an authorised representative.<br>2. The obligations laid down in Article 13(1) to (11), Article 13(12), first subparagraph, and Article 13(14) shall not form part of the authorised representative’s mandate.<br>3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The authorised representative shall provide a copy of the mandate to the market surveillance authorities upon request. The mandate shall allow the authorised representative to do at least the following: | | | Article 18<br>**Authorised representatives**<br><br>1. A manufacturer may appoint an authorised representative by written mandate.<br>2. The obligations laid down in point 1 to 11 of Article 13, the first subpoint of point 12 of article 13, and point 14 of article 13 shall not form part of the authorised representative’s mandate.<br>3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. Upon request, the authorised representative shall provide a copy of the mandate to the market surveillance authorities. The mandate | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | (a) keep the EU declaration of conformity referred to in Article 28 and the technical documentation referred to in Article 31 at the disposal of the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer;<br>(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;<br>(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. | | | shall allow the authorised representative to do at least the following:<br>a. to keep the EU declaration of conformity referred to in article 28 of this law and the technical documentation referred to in article 31 of this law available to the market surveillance responsible structure s for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer;<br>b. following a reasoned request from a market surveillance responsible structure , to provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;<br>c. to cooperate with the market surveillance authorities, at their request, on any action taken to eliminate risks posed by a product with digital elements covered by the authorised representative's mandate. | | |
| **A19** | Article 19<br>**Obligations of importers**<br><br>1. Importers shall place on the market only products with digital elements that comply with the essential cybersecurity requirements set out in Part I of Annex I and where the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.<br>2. Before placing a product with digital elements on the market, importers shall ensure that:<br>(a) the appropriate conformity assessment procedures as referred to in Article 32 have been carried out by the manufacturer;<br>(b) the manufacturer has drawn up the technical documentation;<br>(c) the product with digital elements bears the CE marking referred to in Article 30 and is accompanied by the EU declaration of conformity referred to in Article 13(20) and the information and instructions to the user as set out in Annex II in a language which can be easily understood by users and market surveillance authorities;<br>(d) the manufacturer has complied with the requirements set out in Article 13(15), (16) and (19).<br>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.<br>3. Where an importer considers or has reason to believe that a product with digital elements or the | | **A19** | Article 19<br>**Obligations of importers**<br><br>1. Importers shall place on the market only products with digital elements that comply with the essential cybersecurity requirements set out in part I of annex I to this law and for which the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in part II of annex I to this law.<br>2. Before placing a product with digital elements on the market, importers shall ensure that:<br>a. the appropriate conformity assessment procedures referred to in article 32 of this law have been carried out by the manufacturer;<br>b. the manufacturer has drawn up the technical documentation;<br>c. the product with digital elements bears the CE marking referred to in article 30 of this law and is accompanied by the EU declaration of conformity referred to in point 20 of article 13 of this law and the user information and instructions referred to in annex II to this law, in a language easily understood by users and the market surveillance authorities;<br>ç. the manufacturer has complied with the requirements laid down in points 15, 16 and 19 of article 13 of this law.<br>For the purposes of this point, importers shall be able to provide the necessary documents | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | processes put in place by the manufacturer are not in conformity with this Regulation, 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 this Regulation. 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.<br>Where an importer has reason to believe that a product with digital elements may present a significant cybersecurity risk in light of non-technical risk factors, the importer shall inform the market surveillance authorities to that effect. Upon receipt of such information, the market surveillance authorities shall follow the procedures referred to in Article 54(2).<br>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 at which they can be contacted on the product with digital elements or 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.<br>5. Importers who know or have reason to believe that a product with digital elements which they have placed on the market is not in conformity with this Regulation shall immediately take the corrective measures necessary to ensure that the product with digital elements is brought into conformity with this Regulation, or to withdraw or recall the product, if appropriate.<br>Upon becoming aware of 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 have made the product with digital elements available on the market to that effect, giving details, in particular, of non-compliance and of any corrective measures taken.<br>6. Importers shall, for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and | | | demonstrating compliance with the requirements laid down in this article.<br>3. Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer do not comply with this law, the importer shall not place the product on the market until the product or the processes put in place by the manufacturer have been brought into conformity with this law. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance responsible structure s accordingly.<br>Where an importer has reason to believe that a product with digital elements may present a significant cybersecurity risk, taking into account non-technical risk factors, the importer shall inform the market surveillance responsible structure s accordingly. Upon receiving such information, the market surveillance responsible structure s shall follow the procedures referred to in point 2 of article 51 of this law.<br>4. Importers shall indicate their name, registered trade name or registered trademark, postal address, email address or other digital contact details and, where applicable, the website through which they can be contacted, on the product with digital elements, its packaging or a document accompanying the product. The contact details shall be provided in a language easily understood by users and the market surveillance authorities.<br>5. Importers who know or have reason to believe that a product with digital elements they have placed on the market does not comply with this law shall immediately take the necessary corrective measures to bring the product into conformity with this law or, where appropriate, to withdraw or recall it.<br>Upon becoming aware of a vulnerability in a product with digital elements, importers shall immediately inform the manufacturer of that vulnerability. Furthermore, where the product presents a significant cybersecurity risk, importers shall immediately inform the market surveillance responsible structure s in whose territory they made the product available on the market, providing details, in particular, of the non-compliance and any corrective measures taken. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | ensure that the technical documentation can be made available to those authorities, upon request.<br>7. 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 cybersecurity requirements set out in Part I of Annex I as well as of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II 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.<br>8. Where the importer of a product with digital elements becomes aware that the manufacturer of that product has 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. | | | 6. For at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, importers shall keep a copy of the EU declaration of conformity available to the market surveillance responsible structure s and shall ensure that the technical documentation can be made available to the authorities upon request.<br>7. At the reasoned request of a market surveillance responsible structure , importers shall provide all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential cybersecurity requirements set out in Part I of annex I to this law, and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in part II of annex I to this law, in a language that can be easily understood by the authorities. At their request, importers shall cooperate with the authorities on any action taken to eliminate cybersecurity risks posed by a product with digital elements that they have placed on the market.<br>8. Where the importer of a product with digital elements becomes aware that the manufacturer of that product has ceased its operations and, as a result, is unable to fulfil the obligations laid down in this law, the importer shall inform the market surveillance responsible structure s of that situation and, by any available means and to the extent possible, users of the products with digital elements placed on the market. | | |
| **A20** | Article 20<br>**Obligations of distributors**<br><br>1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements set out in this Regulation.<br>2. Before making a product with digital elements available on the market, distributors shall verify that:<br>(a) the product with digital elements bears the CE marking;<br>(b) the manufacturer and the importer have complied with the obligations set out in Article 13(15), (16), (18), (19) and (20) and Article 19(4), and have provided all necessary documents to the distributor. | | **A20** | Article 20<br>**Obligations of distributors**<br><br>1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements laid down in this law.<br>2. Before making a product with digital elements available on the market, distributors shall verify that:<br>a. the product with digital elements bears the CE marking;<br>b. the manufacturer and the importer have complied with the obligations laid down in points 15, 16, 18, 19 and 20 of Article 13 and point 4 of article 19 of this law and have provided the distributor with all the necessary documents. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 3. Where a distributor considers or has reason to believe, on the basis of information in its possession, that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity 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 with this Regulation. 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.<br>4. Distributors who know or have reason to believe, on the basis of information in their possession, 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 this Regulation 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, or to withdraw or recall the product, if appropriate, are taken.<br>Upon becoming aware of a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken.<br>5. Distributors shall, further to a reasoned request from a market surveillance authority, provide 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 this Regulation 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.<br>6. Where the distributor of a product with digital elements becomes aware, on the basis of information in its possession, that the manufacturer of that product has ceased its operations and, as result, is | | | 3. Where a distributor considers or has reason to believe, on the basis of the information in its possession, that a product with digital elements or the processes put in place by the manufacturer do not comply with the essential cybersecurity requirements set out in annex I to this law, the distributor shall make the product with digital elements available on the market until the product or the processes put in place by the manufacturer have been brought into conformity with this law. Furthermore, where the product presents a significant cybersecurity risk, the distributor shall immediately inform the manufacturer and the market surveillance responsible structure s accordingly.<br>4. Distributors who know or have reason to believe, on the basis of the information in their possession, that a product with digital elements they have made available on the market, or the processes put in place by its manufacturer, do not comply with this law shall ensure that the necessary corrective measures are taken to bring the product or those processes into conformity, or, where appropriate, to withdraw or recall the product.<br>Upon becoming aware of a vulnerability in a product with digital elements, distributors shall immediately inform the manufacturer of that vulnerability. Furthermore, where the product presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance authorities, providing details, in particular, of the non-compliance and any corrective measures taken.<br>5. At the reasoned request of a market surveillance responsible structure , distributors shall provide 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 this law, in a language that can be easily understood by the authorities. At their request, distributors shall cooperate with the authorities on any action taken to eliminate cybersecurity risks posed by a product with digital elements that they have made available on the market.<br>6. Where a distributor of a product with digital elements becomes aware, on the basis of information in its possession, that the manufacturer of that product has ceased its operations and, as a result, is unable to fulfil the obligations laid down in this law, the distributor shall immediately inform the market surveillance responsible structure s of that | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 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. | | | situation and, by any available means and to the extent possible, users of the products with digital elements placed on the market. | | |
| **A21** | Article 21<br>**Cases in which obligations of manufacturers apply to importers and distributors**<br><br>An importer or distributor shall be considered to be a manufacturer for the purposes of this Regulation and shall be subject to Articles 13 and 14, where that importer or distributor places a product with digital elements on the market under its name or trademark or carries out a substantial modification of a product with digital elements already placed on the market. | | **A21** | Article 21<br>**Cases in which the obligations of manufacturers apply to importers and distributors**<br><br>An importer or distributor shall be considered a manufacturer for the purposes of this law and shall be subject to articles 13 and 14 where that importer or distributor places a product with digital elements on the market under its own name or trademark, or carries out a substantial modification of a product with digital elements already placed on the market. | **F** | |
| **A22** | Article 22<br>**Other cases in which obligations of manufacturers apply**<br><br>1. A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of a product with digital elements and makes that product available on the market, shall be considered to be a manufacturer for the purposes of this Regulation.<br>2. The person referred to in paragraph 1 of this Article shall be subject to the obligations set out in Articles 13 and 14 for the part of the product with digital elements 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. | | **A22** | Article 22<br>**Other cases in which the obligations of manufacturers apply**<br><br>1. A natural or legal person, other than the manufacturer, importer or distributor, who carries out a substantial modification of a product with digital elements and makes that product available on the market shall be considered a manufacturer for the purposes of this law.<br>2. The person referred to in point 1 of this article shall be subject to the obligations laid down in articles 13 and 14 of this law in respect of the part of the product with digital elements affected by the substantial modification or, where the substantial modification affects the cybersecurity of the product with digital elements as a whole, in respect of the entire product. | **F** | |
| **A23** | Article 23<br>**Identification of economic operators**<br><br>1. Economic operators shall, on request, provide the market surveillance authorities with the following information:<br>(a) the name and address of any economic operator who has supplied them with a product with digital elements;<br>(b) where available, the name and address of any economic operator to whom they have supplied a product with digital elements. | | | Article 23<br>**Identification of economic operators**<br><br>1. Upon request, economic operators shall provide the market surveillance responsible structure s with the following information:<br>the name and address of any economic operator that supplied them with a product with digital elements;<br>where available, the name and address of any economic operator to whom they supplied a product with digital elements.<br>2. Economic operators shall be able to present the information referred to in point 1 of this | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 2. Economic operators shall be able to present the information referred to in paragraph 1 for 10 years after they have been supplied with the product with digital elements and for 10 years after they have supplied the product with digital elements. | | | article for 10 years after they were supplied with the product with digital elements and for 10 years after they supplied products with digital elements. | | |
| **A24** | Article 24<br>**Obligations of open-source software stewards**<br><br>1. Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject. That policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community.<br>2. Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software.<br>Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.<br>3. The obligations laid down in Article 14(1) shall apply to open-source software stewards to the extent that they are involved in the development of the products with digital elements. The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products. | | | Article 24<br>**Obligations of open-source software stewards**<br><br>1. Open-source software stewards shall establish and document, in a verifiable manner, a cybersecurity policy to promote the development of a secure product with digital elements and effective vulnerability handling by the developers of that product. That policy shall also promote voluntary reporting of vulnerabilities by developers of the product, as provided for in article 15, and shall take account of the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject. In particular, the policy shall address the documentation, handling and remediation of vulnerabilities and promote the sharing within the open-source community of information about vulnerabilities discovered.<br>2. At their request, open-source software stewards shall cooperate with the market surveillance responsible structure s in order to mitigate cybersecurity risks posed by a product with digital elements that qualifies as free and open-source software. At the reasoned request of a market surveillance responsible structure , open-source software stewards shall provide that authority, in a language it can easily understand and in paper or electronic form, with the documentation referred to in point 1 of this Article.<br>3. The obligations laid down in point 1 of article 14 shall apply to open-source software stewards to the extent that they are involved in the development of products with digital elements. The obligations laid down in points 3 and 8 of Article 14 shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect the network and information systems that those stewards provide for the development of such products. | **F** | |
| **A25** | Article 25<br>**Security attestation of free and open-source software** | | **A25** | Article 25<br>**Attestation of security of free and open-source software** | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | In order to facilitate the due diligence obligation set out in Article 13(5), in particular as regards manufacturers that integrate free and open-source software components in their products with digital elements, the Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by establishing voluntary security attestation programmes allowing the developers or users of products with digital elements qualifying as free and open-source software as well as other third parties to assess the conformity of such products with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation. | | | In order to facilitate compliance with the due diligence obligation laid down in point 5 of article 13, in particular for manufacturers integrating free and open-source software components into their products with digital elements, the Council of Ministers shall, on a proposal from the minister responsible for electronic and digital communications, approve voluntary security attestation programmes. Those programmes shall enable developers or users of products with digital elements that qualify as free and open-source software, as well as other third parties, to assess the conformity of those products with all or some of the essential cybersecurity requirements or other obligations laid down in this law. | | |
| **A26** | Article 26<br>**Guidance**<br><br>1. In order to facilitate implementation and ensure the consistency of such implementation, the Commission shall publish guidance to assist economic operators in applying this Regulation, with a particular focus on facilitating compliance by microenterprises and small and medium-sized enterprises.<br>2. Where it intends to provide guidance as referred to in paragraph 1, the Commission shall address at least the following aspects:<br>(a) the scope of this Regulation, with a particular focus on remote data processing solutions and free and open-source software;<br>(b) the application of support periods in relation to particular categories of products with digital elements;<br>(c) guidance targeted at manufacturers subject to this Regulation that are also subject to Union harmonisation legislation other than this Regulation or to other related Union legal acts;<br>(d) the concept of substantial modification.<br>The Commission shall also maintain an easy-to-access list of the delegated and implementing acts adopted pursuant to this Regulation.<br>3. When preparing the guidance pursuant to this Article, the Commission shall consult relevant stakeholders. | | **A26** | Article 26<br>**Guidance**<br><br>1. In order to facilitate and ensure consistent implementation of this law, the minister responsible for the economy and the minister responsible for digitalisation shall, also taking into account suggestions from the authority responsible for cybersecurity and the authority responsible for e-government, approve joint guidance to assist economic operators in implementing this law, with particular emphasis on facilitating compliance by microenterprises and small and medium-sized enterprises.<br>2. For the purposes of providing the guidance referred to in point 1 of this article, the responsible minister shall address at least the following aspects:<br>a. the scope of this law, with particular emphasis on remote data processing solutions and free and open-source software;<br>b. the application of support periods to specific categories of products with digital elements;<br>c. guidance for manufacturers subject to this law who are also subject to other relevant legislation in force;<br>ç. the concept of substantial modification.<br>3. When preparing the guidance under this article, the responsible minister shall consult the relevant interested parties. | **F** | |
| **A27** | Article 27<br>**Presumption of conformity** | | **A27** | Article 27<br>**Presumption of conformity** | **F** | Points 1 and 2 of Article 27 of the Regulation apply partially, whereas |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof, the references of which have been published in the Official Journal of the European Union, shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I covered by those standards or parts thereof.<br>The Commission shall, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the essential cybersecurity requirements set out in Annex I to this Regulation. When preparing standardisation requests for this Regulation, the Commission shall strive to take into account existing European and international standards for cybersecurity that are in place or under development in order to simplify the development of harmonised standards, in accordance with Regulation (EU) No 1025/2012.<br>2. The Commission may adopt implementing acts establishing common specifications covering technical requirements that provide a means to comply with the essential cybersecurity requirements set out in Annex I for products with digital elements that fall within the scope of this Regulation.<br>Those implementing acts shall be adopted only where the following conditions are fulfilled:<br>(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 cybersecurity requirements set out in Annex I and:<br>(i) the request has not been accepted;<br>(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<br>(iii) the harmonised standards do not comply with the request; and<br>(b) no reference to harmonised standards covering the relevant essential cybersecurity requirements set out in Annex I to this Regulation 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.<br>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). | | | 1. Products with digital elements and the processes put in place by the manufacturer that comply with harmonised standards, or parts thereof, the references of which have been published in the Official Gazette, shall be presumed to comply with the essential cybersecurity requirements set out in annex I to this law covered by those standards or parts thereof.<br>On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall approve lists of harmonised standards, in accordance with the relevant European harmonised standards, for the essential cybersecurity requirements set out in annex I to this law.<br>2. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall approve common specifications covering technical requirements that provide a means of complying with the essential cybersecurity requirements set out in annex I for products with digital elements falling within the scope of this law, in accordance with relevant European Commission practice.<br>3. Products with digital elements and the processes put in place by the manufacturer that comply with the common specifications adopted by the acts referred to in point 2 of this article, or parts thereof, shall be presumed to comply with the essential cybersecurity requirements set out in annex I covered by those common specifications or parts thereof.<br>4. Products with digital elements and the processes put in place by the manufacturer for which an EU declaration of conformity or a certificate under a cybersecurity certification scheme adopted pursuant to the legislation in force on cybersecurity, or under a European cybersecurity certification scheme, has been issued shall be presumed to comply with the essential cybersecurity requirements set out in annex I to this law to the extent that the EU declaration of conformity or cybersecurity certificate, or parts thereof, cover those requirements.<br>5. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall specify the adopted cybersecurity certification schemes that may be used to demonstrate the conformity of products with digital elements with the essential cybersecurity requirements, or parts thereof, set out in annex I to this law. The issuance of a cybersecurity certificate under those schemes at an assurance level of at least “substantial” shall remove | | points 3, 4, 6, and 7 of Article 27 of the Regulation concern Member States and are inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 3. Before preparing the draft implementing act referred to in paragraph 2 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers that the conditions in paragraph 2 of this Article have been fulfilled.<br>4. When preparing the draft implementing act referred to in paragraph 2, the Commission shall take into account the views of relevant bodies and shall duly consult all relevant stakeholders.<br>5. 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 2 of this Article, or parts thereof, shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I covered by those common specifications or parts thereof.<br>6. 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 a 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 2 of this Article, or parts thereof which cover the same essential cybersecurity requirements as those covered by that harmonised standard.<br>7. Where a Member State considers that a common specification does not entirely satisfy the essential cybersecurity requirements set out in Annex I, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.<br>8. 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 pursuant to Regulation (EU) 2019/881 shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I in so far as the EU statement of conformity or European cybersecurity certificate, or parts thereof, cover those requirements.<br>9. The Commission is empowered to adopt delegated acts in accordance with Article 61 of this | | | the manufacturer's obligation to carry out a third-party conformity assessment for the relevant requirements, as provided for in letters a) and b) of point 2 of article 32 and letters a) and b) of point 3 of article 32 and (b) of this law. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Regulation to supplement this Regulation by specifying the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity of products with digital elements with the essential cybersecurity requirements or parts thereof as set out in Annex I to this Regulation. Furthermore, the issuance of a European cybersecurity certificate issued under such schemes, at least at assurance level 'substantial', eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 32(2), points (a) and (b), and Article 32(3), points (a) and (b), of this Regulation | | | | | |
| **A28** | Article 28<br>**EU declaration of conformity**<br><br>1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 13(12) and state that the fulfilment of the applicable essential cybersecurity requirements set out in Annex I has been demonstrated.<br>2. The EU declaration of conformity shall have the model structure set out in Annex V and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VIII. Such a declaration shall be updated as appropriate. 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.<br>The simplified EU declaration of conformity referred to in Article 13(20) shall have the model structure set out in Annex VI. 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.<br>3. Where a product with digital elements is subject to more than one Union legal act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union legal acts. That declaration shall contain the identification of the Union legal acts concerned, including their publication references.<br>4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product with digital elements.<br>5. The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by adding elements to the | | | Article 28<br>**EU declaration of conformity**<br><br>1. Manufacturers shall draw up the EU declaration of conformity in accordance with point 12 of article 13 of this law and shall declare that compliance with the applicable essential cybersecurity requirements set out in annex I to this law has been demonstrated.<br>2. The EU declaration of conformity shall follow the model structure set out in annex V and contain the elements specified in the relevant conformity assessment procedures set out in annex VIII to this law. It shall be kept up to date, as appropriate, and made available in Albanian. The simplified EU declaration of conformity referred to in point 20 of article 13 of this law shall follow the model structure set out in annex VI to this law. It shall be made available in Albanian.<br>3. Where a product with digital elements is subject to one or more legal acts requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such legal acts. That declaration shall list the legal acts concerned, including their publication references.<br>4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the conformity of the product with digital elements.<br>5. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall approve additional elements to be included in the minimum content of the EU declaration of conformity set out in annex V to this law, to take | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | minimum content of the EU declaration of conformity set out in Annex V to take account of technological developments. | | | account of technological developments in accordance with relevant European Union practice. | | |
| **A29** | Article 29<br>**General principles of the CE marking**<br><br>The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008. | | **A29** | **Article 29**<br>**General principles of the CE marking**<br><br>The CE marking shall be subject to the general principles laid down in the legislation in force on accreditation relating to the advertising of products. | **F** | |
| **A30** | Article 30<br>**Rules and conditions for affixing the CE marking**<br><br>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 28 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 28 or on the website accompanying the software product. In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.<br>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.<br>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 cybersecurity risk or use set out in the implementing acts referred to in paragraph 6.<br>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 32.<br>The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised representative.<br>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. | | **A30** | Article 30<br>**Rules and conditions for affixing the CE marking**<br><br>1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or cannot be ensured due to the nature of the product, it shall be affixed to the packaging and to the EU declaration of conformity referred to in article 28 of this law accompanying the product. For products with digital elements in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in article 28 of this law or to the website accompanying the software product. In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.<br>2. Due to the nature of the product with digital elements, the height of the CE marking affixed to the product may be less than 5 mm, provided that it remains visible and legible.<br>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 other indication of a specific cybersecurity risk or use, as laid down in the secondary legislation referred to in point 6 of this article.<br>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 set out in annex VIII to this law) referred to in article 32 of this law.<br>The notified body shall affix its identification number itself or, in accordance with its instructions, the manufacturer or the manufacturer's authorised representative shall affix it.<br>5. The affixing of the CE marking to products with digital elements shall build on existing | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Where the product with digital elements is subject to Union harmonisation legislation, other than this Regulation, which also provides for the affixing of the CE marking, the CE marking shall indicate that the product also fulfils the requirements set out in such other Union harmonisation legislation.<br>6. The Commission may, by means of implementing acts, lay down technical specifications for labels, pictograms or any other marks related to the security of the products with digital elements, their support periods and mechanisms to promote their use and to increase public awareness about the security of products with digital elements. When preparing the draft implementing acts, the Commission shall consult relevant stakeholders, and, if it has already been established pursuant to Article 52(15), ADCO. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). | | | mechanisms to ensure the correct application of the regime governing the CE marking, and appropriate action shall be taken in cases of improper use of that marking. Where a product with digital elements is subject to legislation other than this law that also provides for the affixing of the CE marking, the CE marking shall indicate that the product also complies with the requirements laid down in that other relevant legislation in force.<br>6. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall approve technical specifications for labels, pictograms or other markings relating to the security of products with digital elements and their support periods, and mechanisms to promote their use and raise public awareness of the security of products with digital elements. | | |
| **A31** | Article 31<br>**Technical documentation**<br><br>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 cybersecurity requirements set out in Annex I. It shall at least contain the elements set out in Annex VII.<br>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, at least during the support period.<br>3. For products with digital elements as referred to in Article 12, which are also subject to other Union legal acts which provide for technical documentation, a single set of technical documentation shall be drawn up containing the information referred to in Annex VII and the information required by those Union legal acts.<br>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.<br>5. The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by adding elements to be included in the technical documentation set out in Annex VII to take account of technological developments, as | | **A31** | Article 31<br>**Technical documentation**<br><br>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 cybersecurity requirements set out in annex I to this law. The technical documentation shall contain at least the elements set out in annex VII to this law.<br>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, at least throughout the support period.<br>3. For products with digital elements referred to in article 12 of this law that are also subject to other legal acts in force requiring technical documentation, a single set of technical documentation shall be drawn up containing the information referred to in annex VII to this law and the information required by those legal acts.<br>4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in Albanian.<br>5. On a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall approve additional elements to be included in the technical documentation set out in annex VII to this law, | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | well as developments encountered in the implementation process of this Regulation. To that end, the Commission shall strive to ensure that the administrative burden on microenterprises and small and medium-sized enterprises is proportionate. | | | taking account of technological developments and developments observed during the implementation of this law. For this purpose, the Council of Ministers shall ensure that the administrative burden on microenterprises and small and medium-sized enterprises is proportionate. | | |
| **A32** | Article 32<br>**Conformity assessment procedures for products with digital elements**<br><br>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 cybersecurity requirements set out in Annex I are met. The manufacturer shall demonstrate conformity with the essential cybersecurity requirements by using any of the following procedures:<br>(a) the internal control procedure (based on module A) set out in Annex VIII;<br>(b) the EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII;<br>(c) a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; or<br>(d) where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9).<br>2. Where, in assessing the compliance of an important product with digital elements that falls under class I as set out in Annex III and the processes put in place by its manufacturer with the essential cybersecurity requirements set out in Annex I, the manufacturer has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes at assurance level at least 'substantial' as referred to in Article 27, 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 cybersecurity requirements to either of the following procedures:<br>(a) the EU-type examination procedure (based on module B) set out in Annex VIII followed by | | **A32** | Article 32<br>**Conformity assessment procedures for products with digital elements**<br><br>1. The manufacturer shall carry out a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential cybersecurity requirements set out in annex I to this law are met. The manufacturer shall demonstrate conformity with the essential cybersecurity requirements by using one of the following procedures:<br>a. the internal control procedure (based on Module A) set out in annex VIII to this law;<br>b. the EU-type examination procedure (based on Module B) set out in annex VIII to this law, followed by conformity to EU type based on internal production control (based on Module C) set out in annex VIII to this law;<br>c. the conformity assessment based on full quality assurance (based on Module H) set out in annex VIII to this law; or<br>ç. where available and applicable, a cybersecurity certification scheme in accordance with point 9 of article 27 of this law.<br>2. Where, in assessing the conformity of an important product with digital elements falling within class I as set out in annex III to this law, and of the processes put in place by its manufacturer, with the essential cybersecurity requirements set out in annex I to this law, the manufacturer has not applied, or has applied only in part, harmonised standards, common specifications or cybersecurity certification schemes at an assurance level of at least "substantial" as referred to in article 27 of this law, or where such harmonised standards, common specifications or cybersecurity certification schemes do not exist, the product with digital elements and the processes put in place by the manufacturer shall be assessed against those essential cybersecurity requirements using one of the following procedures: | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | conformity to EU-type based on internal production control (based on module C) set out in Annex VIII; or<br>(b) a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII.<br>3. Where the product is an important product with digital elements that falls under class II as set out in Annex III, the manufacturer shall demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using any of the following procedures:<br>(a) EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII;<br>(b) a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; or<br>(c) where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9) of this Regulation at assurance level at least 'substantial' pursuant to Regulation (EU) 2019/881.<br>4. Critical products with digital elements listed in Annex IV shall demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using one of the following procedures:<br>(a) a European cybersecurity certification scheme in accordance with Article 8(1); or<br>(b) where the conditions in Article 8(1) are not met, any of the procedures referred to in paragraph 3 of this Article.<br>5. Manufacturers of products with digital elements qualifying as free and open-source software, which fall under the categories set out in Annex III, shall be able to demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using one of the procedures referred to in paragraph 1 of this Article, provided that the technical documentation referred to in Article 31 is made available to the public at the time of the placing on the market of those products.<br>6. The specific interests and needs of microenterprises and small and medium-sized enterprises, including start-ups, shall be taken into account when setting the fees for conformity assessment procedures and those fees shall be reduced proportionately to their specific interests and needs. | | | a. the EU-type examination procedure (based on Module B) set out in annex VIII to this law, followed by conformity to EU type based on internal production control (based on Module C) set out in annex VIII to this law;<br>b. a conformity assessment based on full quality assurance (based on Module H) set out in annex VIII to this law.<br>3. Where the product is an important product with digital elements falling within class II as set out in annex III to this law, the manufacturer shall demonstrate conformity with the essential cybersecurity requirements set out in annex I to this law by using one of the following procedures:<br>a. the EU-type examination procedure (based on Module B) set out in annex VIII to this law, followed by conformity to EU type based on internal production control (based on Module C) set out in annex VIII to this law;<br>b. a conformity assessment based on full quality assurance (based on Module H) set out in annex VIII to this law;<br>c. where available and applicable, a cybersecurity certification scheme in accordance with point 9 of article 27 of this law at an assurance level of at least "substantial" under the legislation in force on cybersecurity.<br>4. Critical products with digital elements listed in annex IV to this law shall demonstrate conformity with the essential cybersecurity requirements set out in annex I to this law by using one of the following procedures:<br>a. a cybersecurity certification scheme in accordance with point 1 of article 8 of this law;<br>b. where the conditions in point 1 of article 8 of this law are not met, one of the procedures referred to in point 3 of this article.<br>5. Manufacturers of products with digital elements that qualify as free and open-source software and fall within the categories set out in annex III to this law may demonstrate conformity with the essential cybersecurity requirements set out in annex I to this law by using one of the procedures referred to in point 1 of this article, provided that the technical documentation referred to in article 31 of this law is made publicly available when those products are placed on the market.<br>6. The specific interests and needs of microenterprises and small and medium-sized enterprises, including start-ups, shall be taken into | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | account when setting fees for conformity assessment procedures, and those fees shall be reduced proportionately to their specific interests and needs. | | |
| **A33** | Article 33<br>**Support measures for microenterprises and small and medium-sized enterprises, including start-ups**<br><br>1. Member States shall, where appropriate, undertake the following actions, tailored to the needs of microenterprises and small enterprises:<br>(a) organise specific awareness-raising and training activities about the application of this Regulation;<br>(b) establish a dedicated channel for communication with microenterprises and small enterprises and, as appropriate, local public authorities to provide advice and respond to queries about the implementation of this Regulation;<br>(c) support testing and conformity assessment activities, including where relevant with the support of the European Cybersecurity Competence Centre.<br>2. Member States may, where appropriate, establish cyber resilience regulatory sandboxes. Such regulatory sandboxes shall provide for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with this Regulation for a limited period of time before the placing on the market. The Commission and, where appropriate, ENISA, may provide technical support, advice and tools for the establishment and operation of regulatory sandboxes. The regulatory sandboxes shall be set up under the direct supervision, guidance and support by the market surveillance authorities. Member States shall inform the Commission and the other market surveillance authorities of the establishment of a regulatory sandbox through ADCO. The regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. Member States shall ensure open, fair, and transparent access to regulatory sandboxes, and in particular facilitate access by microenterprises and small enterprises, including start-ups.<br>3. In accordance with Article 26, the Commission shall provide guidance for microenterprises and small and medium-sized enterprises in relation to the implementation of this Regulation. | | **A33** | Article 33<br>**Support measures for microenterprises and small and medium-sized enterprises, including start-ups**<br><br>1. Where appropriate, the ministry responsible for the economy shall take the following actions, tailored to the needs of microenterprises and small enterprises:<br>a. organise specific awareness-raising and training activities on the implementation of this law;<br>b. establish a dedicated communication channel for microenterprises and small enterprises and, where appropriate, local public authorities, to provide advice and respond to requests for information on the implementation of this law;<br>c. support testing and conformity assessment activities, including, where necessary, with the support of the European Cybersecurity Competence Centre.<br>2. The ministry responsible for the economy may, in cooperation with other competent authorities, establish regulatory cyber-resilience sandboxes. Those regulatory sandboxes shall provide controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing, with a view to complying with this law for a limited period before the products are placed on the market. Regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. The competent authorities shall ensure open, fair and transparent access to the regulatory sandboxes and, in particular, facilitate access for microenterprises and small enterprises, including start-ups.<br>3. In accordance with article 26 of this law, the minister responsible for the economy shall provide guidance to microenterprises and small and medium-sized enterprises on the implementation of this law.<br>4. Microenterprises and small enterprises may provide all the elements of the technical documentation specified in annex VII to this law using a simplified format. For this purpose, the Council of Ministers shall, on a proposal from the minister responsible for electronic and digital | **F** | Paragraph 2 of the article is partially applicable, whereas paragraph 4 of Article 33 of the regulation concerns Member States and is inapplicable to Albania. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 4. The Commission shall advertise available financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and small enterprises.<br>5. Microenterprises and small enterprises may provide all elements of the technical documentation specified in Annex VII by using a simplified format. For that purpose, the Commission shall, by means of implementing acts, specify the simplified technical documentation form targeted at the needs of microenterprises and small enterprises, including how the elements set out in Annex VII are to be provided. Where a microenterprise or small enterprise opts to provide the information set out in Annex VII in a simplified manner, it shall use the form referred to in this paragraph. Notified bodies shall accept that form for the purposes of conformity assessment.<br>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). | | | communications, approve a simplified technical documentation form tailored to the needs of microenterprises and small enterprises, including how the elements set out in annex VII to this law are to be provided. Where a microenterprise or small enterprise chooses to provide the information specified in annex VII to this law in a simplified manner, it shall use the form referred to in this point. Notified bodies shall accept that form for conformity assessment purposes. | | |
| **A34** | Article 34<br>**Mutual recognition agreements**<br><br>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 third countries, in accordance with Article 218 TFEU, in order to promote and facilitate international trade. | | **A34** | Article 34<br>**Mutual recognition agreements**<br><br>Taking into account the level of technical development and the approach to conformity assessment in another State, the Republic of Albania may conclude mutual recognition agreements with other States, in accordance with the legislation in force, in order to promote and facilitate international trade. | **F** | |
| **A35** | Article 35<br>**Notification**<br><br>1. Member States shall notify the Commission and the other Member States of bodies authorised to carry out conformity assessments in accordance with this Regulation.<br>2. Member States shall strive to ensure, by 11 December 2026 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. | | **A35** | Article 35<br>**Notification**<br><br>Upon accession to the European Union, the notifying authority shall notify the Commission and the other Member States of the bodies authorised to carry out conformity assessments in accordance with this law. | **F** | Article 35, Paragraph 2 of the regulation is binding on the Member States and is not applicable. |
| **A36** | Article 36<br>**Notifying authorities**<br><br>1. Each Member State shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the | | **A36** | Article 36<br>**Notifying authorities**<br>1. The Notifying Authority shall be designated by a decision of the Council of Ministers and shall be responsible for establishing and carrying out the necessary procedures for the assessment, | **F** | Point 2 of Article 36 of the regulation is not applicable, as assuming new functions as a notifying authority could create an overlap |

| | | | | | | |
|---|---|---|---|---|---|---|
| | assessment, designation and notification of conformity assessment bodies and their monitoring, including compliance with Article 41.<br>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.<br>3. Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 of this Article to a body which is not a governmental entity, that body shall be a legal entity and shall comply mutatis mutandis with Article 37. In addition, it shall have arrangements in place to cover liabilities arising from its activities.<br>4. The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3. | | | designation and notification of conformity assessment bodies, as well as for monitoring them, including compliance with article 41 of this law.<br>2. Where the Notifying Authority delegates or entrusts the assessment, notification or monitoring referred to in point 1 of this article to a body that is not a government institution, that body shall be a legal person and shall comply, to the extent possible, with the requirements of article 37 of this law. In addition, the body shall have arrangements in place to cover the liabilities arising from its activities.<br>3. The Notifying Authority shall retain full responsibility for the tasks performed by the body referred to in point 2 of this article. | | of competencies or a conflict of interest for the accreditation body. |
| **A37** | Article 37<br>**Requirements relating to notifying authorities**<br><br>1. A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs.<br>2. A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities.<br>3. A notifying authority shall be organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment.<br>4. A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis.<br>5. A notifying authority shall safeguard the confidentiality of the information it obtains.<br>6. A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks. | | **A37** | Article 37<br>**Requirements for notifying authorities**<br><br>1. The notifying authority shall be established in such a way as to avoid any conflict of interest with conformity assessment bodies.<br>2. The notifying authority shall be organised and operated so as to safeguard the objectivity and impartiality of its activities.<br>3. The notifying authority shall be organised in such a way that each decision relating to the notification of a conformity assessment body is taken by competent persons other than those who carried out the assessment.<br>4. The notifying authority shall not offer or carry out any activity carried out by conformity assessment bodies, or provide consultancy services on a commercial or competitive basis.<br>5. The notifying authority shall safeguard the confidentiality of the information it receives.<br>6. The notifying authority shall have a sufficient number of competent personnel available for the proper performance of its tasks. | **F** | |
| **A38** | Article 38<br>**Information obligation on notifying authorities**<br><br>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.<br>2. The Commission shall make the information referred to in paragraph 1 publicly available. | | **A38** | Article 38<br>**Information obligation of the notifying authority**<br><br>1. Upon accession to the European Union, the notifying authority shall inform the Commission of the procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes to those procedures. | | Article 38, paragraph 2 of the regulation is binding on the Member States and is inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A39** | Article 39<br>**Requirements relating to notified bodies**<br><br>1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12.<br>2. A conformity assessment body shall be established under national law and have legal personality.<br>3. A conformity assessment body shall be a third-party body independent of the organisation or the product with digital elements it assesses.<br>A body belonging to a business association or professional federation representing undertakings involved in the design, development, production, provision, assembly, use or maintenance of products with digital elements which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered to be such a third-party body.<br>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.<br>A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, development, production, import, distribution, the marketing, installation, use or maintenance of the products with digital elements which they assess, 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.<br>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.<br>5. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional | | **A39** | Article 39<br>**Requirements for notified bodies**<br><br>1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in points 2 to 12 of this article.<br>2. A conformity assessment body shall be established under the legislation in force on accreditation and shall be a legal person.<br>3. A conformity assessment body shall be an independent third-party body from the organisation or product with digital elements that it assesses.<br>A body belonging to a business or professional association representing undertakings involved in the design, development, manufacture, provision, assembly, use or maintenance of the products with digital elements it assesses may be considered a third-party body, provided that its independence and absence of any conflict of interest are demonstrated.<br>4. The conformity assessment body, its senior management and the personnel responsible for carrying out 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 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 products for personal purposes.<br>The conformity assessment body, its senior management and the personnel responsible for carrying out conformity assessment tasks shall not be directly involved in the design, development, manufacture, import, distribution, marketing, installation, use or maintenance of the products with digital elements they assess, nor 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 the conformity assessment activities for which they are notified. This applies in particular to consultancy services.<br>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.<br>5. Conformity assessment bodies and their personnel shall carry out conformity assessment activities with the highest degree of professional | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 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.<br>6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VIII 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.<br>At all times and for each conformity assessment procedure and each kind or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary:<br>(a) personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;<br>(b) descriptions of procedures in accordance with which conformity assessment is to be carried out, ensuring the transparency of and ability to reproduce 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;<br>(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.<br>A conformity assessment body 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.<br>7. The personnel responsible for carrying out conformity assessment activities shall have the following:<br>(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;<br>(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;<br>(c) appropriate knowledge and understanding of the essential cybersecurity requirements set out in Annex I, of the applicable harmonised standards and | | | integrity and the requisite technical competence in the specific field, and shall be free from all pressure and inducements, particularly financial, that could influence their judgement or the results of their conformity assessment activities, especially in relation to persons or groups of persons with an interest in the results of those activities.<br>6. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in annex VIII to this law and for which it is notified, whether those tasks are performed by the conformity assessment body itself or on its behalf and under its responsibility.<br>At all times, and for each conformity assessment procedure and each type or category of products with digital elements for which it is notified, a conformity assessment body shall have the necessary resources, including:<br>a. personnel with sufficient and appropriate technical knowledge and experience to carry out the conformity assessment tasks;<br>b. descriptions of the procedures in accordance with which conformity assessment is carried out, ensuring transparency and the ability to reproduce those procedures, and appropriate policies and procedures distinguishing between the tasks it performs as a notified body and its other activities;<br>c. procedures for carrying out activities that take into account the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology and the mass or serial nature of the production process.<br>A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities.<br>7. The personnel responsible for carrying out conformity assessment activities shall have:<br>a. technical and vocational training covering all conformity assessment activities in respect of which the conformity assessment body is notified;<br>b. satisfactory knowledge of the requirements of the assessments they carry out and appropriate authority to carry out those assessments;<br>c. appropriate knowledge and understanding of the essential cybersecurity requirements set out in annex I to this law, the | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | common specifications, and of the relevant provisions of Union harmonisation legislation and implementing acts;<br>(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.<br>8. The impartiality of the conformity assessment bodies, their top level management and of the assessment personnel shall be guaranteed.<br>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.<br>9. Conformity assessment bodies shall take out liability insurance unless liability is assumed by their Member State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.<br>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 VIII or any provision of national law giving effect to it, except in relation to the market surveillance authorities of the Member State in which its activities are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.<br>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 51 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group.<br>12. Conformity assessment bodies shall operate in accordance with a set of consistent, fair, proportionate and reasonable terms and conditions, while avoiding unnecessary burden for economic operators, in particular taking into account the interests of microenterprises and small and medium-sized enterprises in relation to fees. | | | applicable harmonised standards and common specifications, and the relevant provisions of other legislation in force and secondary legislation;<br>ç. the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.<br>8. The conformity assessment body, its senior administrative and technical managers, and its conformity assessment personnel shall guarantee impartiality. The remuneration of the senior management and personnel responsible for conformity assessment tasks shall not depend on the number of assessments carried out or on their results.<br>9. A conformity assessment body shall take out civil liability insurance, except where liability for conformity assessment is covered by the State or the State itself is responsible for the conformity assessment.<br>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 VIII to this law or any provision of other legislation in force, except in relation to the market surveillance authorities, while intellectual property rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this point.<br>11. Conformity assessment bodies shall participate in, or ensure that their conformity assessment personnel are informed about, relevant standardisation activities and the activities of the group coordinating notified bodies established under article 48 of this law, and shall apply the decisions and administrative documents produced as a result of that group's work as general guidance.<br>12. Conformity assessment bodies shall operate under a consistent, fair, proportionate and reasonable set of terms and conditions, avoiding unnecessary burdens on economic operators and taking particular account of the interests of microenterprises and small and medium-sized enterprises in relation to fees. | | |
| **A40** | Article 40<br>**Presumption of conformity of notified bodies**<br><br>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 | | **A40** | Article 40<br>**Presumption of conformity of notified bodies**<br><br>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 Gazette and, upon accession to the | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | requirements set out in Article 39 in so far as the applicable harmonised standards cover those requirements. | | | European Union, in the Official Journal of the European Union, it shall be presumed to comply with the requirements laid down in article 39 of this law to the extent that the applicable harmonised standards cover those requirements. | | |
| **A41** | Article 41<br>**Subsidiaries of and subcontracting by notified bodies**<br><br>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 39 and shall inform the notifying authority accordingly.<br>2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever they are established.<br>3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the manufacturer.<br>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. | | **A41** | Article 41<br>**Subsidiaries and subcontracting by notified bodies**<br><br>1. Where a notified body subcontracts specific tasks relating to conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or subsidiary meets the requirements laid down in article 39 of this law and shall inform the notifying authority accordingly.<br>2. Notified bodies shall assume full responsibility for the tasks performed by subcontractors or subsidiaries, wherever they are established.<br>3. Activities may be subcontracted or carried out by a subsidiary only with the manufacturer"s agreement.<br>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 subsidiary and the work carried out by them under this law. | **F** | |
| **A42** | Article 42<br>**Application for notification**<br><br>1. A conformity assessment body shall submit an application for notification to the notifying authority of the Member State in which it is established.<br>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 with digital elements for which that body claims to be competent, as well as, where applicable, by an accreditation certificate issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 39.<br>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 39. | | **A42** | Article 42<br>**Application for notification**<br><br>1. A conformity assessment body shall submit an application for notification to the notifying authority.<br>2. The application shall be accompanied by a description of the conformity assessment activities, the conformity assessment procedure or procedures, and the product or products with digital elements for which the body claims to be competent, and, where applicable, by an accreditation certificate issued by the national accreditation body attesting that the conformity assessment body meets the requirements laid down in article 39 of this law.<br>3. Where the conformity assessment body 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 39 of this law. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A43** | Article 43<br>**Notification procedure**<br><br>1. Notifying authorities shall notify only conformity assessment bodies which have satisfied the requirements laid down in Article 39.<br>2. The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations information system developed and managed by the Commission.<br>3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and product or products with digital elements concerned and the relevant attestation of competence.<br>4. Where a notification is not based on an accreditation certificate as referred to in Article 42(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 39.<br>5. The body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification where an accreditation certificate is used or within two months of a notification where accreditation is not used.<br>Only such a body shall be considered to be a notified body for the purposes of this Regulation.<br>6. The Commission and the other Member States shall be notified of any subsequent relevant changes to the notification. | | **A43** | Article 43<br>**Notification procedure**<br><br>1. The notifying authority shall notify only conformity assessment bodies that have fulfilled the requirements laid down in article 39 of this law.<br>2. Upon accession to the European Union, the notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations Information System developed and managed by the Commission.<br>3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules, and the product or products with digital elements, together with the relevant attestation of competence.<br>4. Where a notification is not based on an accreditation certificate as referred to in point 2 of article 42, upon accession to the European Union the notifying authority shall provide the Commission and the other Member States with documentary evidence attesting to the competence of the conformity assessment body and the arrangements in place to ensure that the body will be regularly monitored and will continue to meet the requirements laid down in article 39.<br>5. Upon accession to the European Union, the notifying body may carry out the activities of a notified body only where no objection is raised by the Commission or the other Member States within two weeks of a notification based on an accreditation certificate, or within two months of a notification where accreditation is not used.<br>Only such a body shall be considered a notified body for the purposes of this law.<br>6. Upon accession to the European Union, the Commission and the other Member States shall be notified of any subsequent relevant changes to the notification. | **F** | |
| **A44** | Article 44<br>**Identification numbers and lists of notified bodies**<br><br>1. The Commission shall assign an identification number to a notified body.<br>It shall assign a single such number even where the body is notified under several Union legal acts.<br>2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that | | | | **N** | Article 44 of the regulation concerns member states and is inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | have been allocated to them and the activities for which they have been notified.<br>The Commission shall ensure that that list is kept up to date. | | | | | |
| **A45** | Article 45<br>**Changes to notifications**<br><br>1. Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 39, 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.<br>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. | | **A44** | Article 44<br>**Changes to notifications**<br><br>1. Where the notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in article 39 of this law, or is failing to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw the notification, as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. Upon accession to the European Union, the notifying authority shall immediately inform the Commission and the other Member States accordingly.<br>2. In the event of restriction, suspension or withdrawal of a notification, or where the notified body has ceased its activity, the notifying authority shall take appropriate steps to ensure that the notified body's files are processed by another notified body or are kept available to the notifying authorities and the market surveillance responsible structure upon their request. | **F** | |
| **A46** | Article 46<br>**Challenge of the competence of notified bodies**<br><br>1. The Commission shall investigate all cases where it doubts, or where doubt is brought to its attention regarding, the competence of a notified body to meet, or the continued fulfilment by a notified body of, the requirements and responsibilities to which it is subject.<br>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.<br>3. The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated confidentially.<br>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. | | | | **N** | Article 46 of the regulation concerns member states and is inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A47** | Article 47<br>**Operational obligations of notified bodies**<br><br>1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 32 and Annex VIII.<br>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 undertakings, in particular as regards microenterprises and small and medium-sized enterprises, the sector in which they operate, their structure, their degree of complexity and the cybersecurity risk level of the products with digital elements and technology in question and the mass or serial nature of the production process.<br>3. Notified bodies shall however respect the degree of rigour and the level of protection required for the compliance of products with digital elements with this Regulation.<br>4. Where a notified body finds that the requirements set out in Annex I or in corresponding harmonised standards or common specifications as referred to in Article 27 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a certificate of conformity.<br>5. Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product with digital elements 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.<br>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. | | **Neni 45** | Article 45<br>**Operational obligations of notified bodies**<br><br>1. Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in article 32 and annex VIII to this law.<br>2. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens on economic operators. Conformity assessment bodies shall carry out their activities taking into account the size of undertakings, in particular microenterprises and small and medium-sized enterprises, the sector in which they operate, their structure, the degree of complexity and the level of cybersecurity risk of the products with digital elements, as well as the technology and the mass or serial nature of the production process.<br>3. Notified bodies shall respect the degree of rigour and the level of protection required for products with digital elements to comply with this law.<br>4. Where a notified body finds that the requirements laid down in annex I to this law, or in the relevant harmonised standards or common specifications referred to in article 27 of this law, have not been met by a manufacturer, it shall require the manufacturer to take appropriate corrective measures and shall not issue a certificate of conformity.<br>5. Where, in the course of monitoring conformity after the issuance of a certificate, a notified body finds that a product with digital elements no longer complies with the requirements laid down in this law, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the certificate if necessary.<br>6. Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any certificate, as appropriate. | **F** | |
| **A48** | Article 48<br>**Appeal against decisions of notified bodies**<br><br>Member States shall ensure that an appeal procedure against decisions of the notified bodies is available. | | **A46** | Article 46<br>**Appeals against decisions of notified bodies**<br><br>The legislation in force shall ensure that an appeal procedure is available against decisions of notified bodies. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A49** | Article 49<br>**Information obligation on notified bodies**<br><br>1. Notified bodies shall inform the notifying authority of the following:<br>(a) any refusal, restriction, suspension or withdrawal of a certificate;<br>(b) any circumstances affecting the scope of and conditions for notification;<br>(c) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;<br>(d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.<br>2. Notified bodies shall provide the other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same products with digital elements with relevant information on issues relating to negative and, upon request, positive conformity assessment results. | | **A47** | Article 47<br>**Information obligation of notified bodies**<br><br>1. Notified bodies shall inform the notifying authority of the following:<br>a. any refusal, restriction, suspension or withdrawal of a certificate;<br>b. any circumstance affecting the scope or conditions of notification;<br>c. any request for information received from the market surveillance responsible structure concerning conformity assessment activities;<br>ç. upon request, conformity assessment activities carried out within the scope of their notification and any other activity carried out, including cross-border activities and subcontracting.<br>2. Notified bodies shall provide other notified bodies under this law carrying out similar conformity assessment activities covering the same products with digital elements with relevant information on matters relating to negative results and, upon request, positive results of conformity assessment. | **F** | |
| **A50** | Article 50<br>**Exchange of experience**<br><br>The Commission shall provide for the organisation of the exchange of experience between the Member States' national authorities responsible for notification policy. | | | | **N** | Article 50 of the regulation concerns member states and is inapplicable. |
| **A51** | Article 51<br>**Coordination of notified bodies**<br><br>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.<br>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. | | **A48** | Article 48<br>**Coordination of notified bodies**<br><br>1. The notifying authority shall facilitate the establishment and operation of appropriate coordination and cooperation between notified bodies in the form of a cross-sectoral group of notified bodies.<br>2. The notifying authority shall ensure that notified bodies participate in the group"s work, either directly or through designated representatives. | **F** | |
| **Neni 52** | Article 52<br>**Market surveillance and control of products with digital elements in the Union market**<br><br>1. Regulation (EU) 2019/1020 shall apply to products with digital elements that fall within the scope of this Regulation. | | **A49** | Article 49<br>**Market surveillance and control of products with digital elements on the internal market** | **F** | Point 15 of Article 52 of the Regulation, concerning adCO, is partially applicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 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.<br>3. The market surveillance authorities designated under paragraph 2 of this Article shall also be responsible for carrying out market surveillance activities in relation to the obligations for open-source software stewards laid down in Article 24. Where a market surveillance authority finds that an open-source software steward does not comply with the obligations set out in that Article, it shall require the open-source software steward to ensure that all appropriate corrective actions are taken. Open-source software stewards shall ensure that all appropriate corrective action is taken in respect of their obligations under this Regulation.<br>4. Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated pursuant to 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 14 of this Regulation, the designated market surveillance authorities shall cooperate and exchange information on a regular basis with the CSIRTs designated as coordinators and ENISA.<br>5. The market surveillance authorities may request a CSIRT designated as coordinator or ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 54, market surveillance authorities may request the CSIRT designated as coordinator or ENISA to provide an analysis to support evaluations of compliance of products with digital elements.<br>6. Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of Union harmonisation legislation other than this Regulation, and exchange information on a regular basis.<br>7. Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing those authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 10 if such guidance and advice concerns the processing of personal data. | | | 1. The legislation in force on market surveillance shall apply to products with digital elements falling within the scope of this law.<br><br>2. The market surveillance responsible structure s shall ensure the effective enforcement of this law.<br><br>3. The market surveillance responsible structure s referred to in point 2 of this article shall be responsible for carrying out market surveillance activities concerning the obligations of open-source software stewards laid down in article 24 of this law. Where a market surveillance responsible structure finds that an open-source software steward does not comply with the obligations laid down in that article, it shall require the steward to ensure that all appropriate corrective action is taken. Open-source software stewards shall ensure that all appropriate corrective action is taken in respect of their obligations under this law.<br><br>4. Where appropriate, the market surveillance responsible structure s shall cooperate and regularly exchange information with the national cybersecurity authority. In relation to the supervision of compliance with the reporting obligations under article 14 of this law, the market surveillance responsible structure s shall cooperate and regularly exchange information with the National CSIRT.<br><br>5. The market surveillance responsible structure s may request technical advice from the National CSIRT on matters relating to the implementation and enforcement of this law. When carrying out a verification under article 51 of this law, the market surveillance responsible structure s may request the National CSIRT to provide an analysis supporting the conformity assessments of products with digital elements.<br><br>6. Where appropriate, the market surveillance responsible structure s shall cooperate and regularly exchange information with other market surveillance responsible structure s designated under specific legislation in force other than this law.<br><br>7. Where appropriate, the market surveillance responsible structure s shall cooperate with the authority responsible for the protection of personal data. Such cooperation shall include informing that authority of any findings relevant to the exercise of its powers, including the issuing of guidance and advice under point 10 of this article | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 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.<br>8. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and technical resources, including, where appropriate, processing automation tools, as well as with human resources with the necessary cybersecurity skills to fulfil their tasks under this Regulation.<br>9. The Commission shall encourage and facilitate the exchange of experience between designated market surveillance authorities.<br>10. Market surveillance authorities may provide guidance and advice to economic operators on the implementation of this Regulation, with the support of the Commission and, where appropriate, CSIRTs and ENISA.<br>11. Market surveillance authorities shall inform consumers of where to submit complaints that could indicate non-compliance with this Regulation, in accordance with Article 11 of Regulation (EU) 2019/1020, and shall provide information to consumers on where and how to access mechanisms to facilitate reporting of vulnerabilities, incidents and cyber threats that may affect products with digital elements.<br>12. Market surveillance authorities shall facilitate, where relevant, the cooperation with relevant stakeholders, including scientific, research and consumer organisations.<br>13. The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law.<br>14. For products with digital elements that fall within the scope of this Regulation which are classified as high-risk AI systems pursuant to Article 6 of Regulation (EU) 2024/1689, the market surveillance authorities designated for the purposes of that Regulation shall be the authorities responsible for market surveillance activities required under this | | | where that guidance or advice concerns the processing of personal data.<br><br>The authority responsible for the protection of personal data shall be entitled to request and access any documentation created or maintained under this law where access to that documentation is necessary for the performance of its tasks. The personal data protection authority shall inform the market surveillance responsible structure s of any such request.<br><br>8. The market surveillance responsible structure s shall be provided with financial and technical resources, including, where appropriate, tools for automated processing, and with human resources having the cybersecurity skills necessary to perform their tasks under this law.<br><br>9. The ministry responsible for the relevant field shall encourage and facilitate the exchange of experience between the market surveillance authorities.<br><br>10. The market surveillance responsible structure s may provide economic operators with guidance and advice on the implementation of this law, with the support of the ministry responsible for the economy and, where appropriate, the National CSIRT.<br><br>11. The market surveillance responsible structure s shall inform consumers where to submit complaints that may indicate non-compliance with this law, in accordance with the legislation in force on market surveillance, and shall provide consumers with information on where and how to access mechanisms to facilitate the reporting of vulnerabilities, incidents and cyber threats that may affect products with digital elements.<br><br>12. Where necessary, the market surveillance responsible structure s shall facilitate cooperation with interested parties, including scientific, research and consumer organisations.<br><br>13. The market surveillance responsible structure s shall report annually to the responsible ministry on the results of their relevant market surveillance activities. They shall immediately report to the responsible ministry and the Competition Authority any information identified during market surveillance activities that may be relevant to the enforcement of the legislation in force on competition protection. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Regulation. The market surveillance authorities designated pursuant to Regulation (EU) 2024/1689 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 14 of this Regulation, with the CSIRTs designated as coordinators and ENISA. Market surveillance authorities designated pursuant to Regulation (EU) 2024/1689 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.<br>15. ADCO shall be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. ADCO shall be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of single liaison offices. ADCO shall also address specific matters related to the market surveillance activities in relation to the obligations placed on open-source software stewards.<br>16. Market surveillance authorities shall monitor how manufacturers have applied the criteria referred to in Article 13(8) when determining the support period of their products with digital elements.<br>ADCO shall publish in a publicly accessible and user-friendly form relevant statistics on categories of products with digital elements, including average support periods, as determined by the manufacturer pursuant to Article 13(8), as well as provide guidance that includes indicative support periods for categories of products with digital elements.<br>Where the data suggests inadequate support periods for specific categories of products with digital elements, ADCO may issue recommendations to market surveillance authorities to focus their activities on such categories of products with digital elements. | | | 14. For products with digital elements falling within the scope of this law that are classified as high-risk artificial intelligence systems under the relevant provisions of the legislation in force on artificial intelligence, the market surveillance responsible structure s designated for the purposes of that legislation shall be responsible for the market surveillance activities required under this law. The market surveillance responsible structure s designated under the legislation in force on artificial intelligence shall, where appropriate, cooperate with the market surveillance responsible structure s designated under this law and, in relation to supervision of compliance with the reporting obligations under article 14 of this law, with the National CSIRT. In particular, the market surveillance responsible structure s designated under the legislation in force on artificial intelligence shall inform the market surveillance responsible structure s designated under this law of any findings relevant to the performance of their tasks relating to the enforcement of this law.<br><br>15. The market surveillance responsible structure s shall monitor how manufacturers have applied the criteria referred to in point 8 of article 13 of this law when determining the support period for their products with digital elements. | | |
| **A53** | Article 53<br>**Access to data and documentation**<br><br>Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential cybersecurity requirements set out in Annex I, the market surveillance authorities shall, upon a reasoned request, 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, | | **A50** | Article 50<br><br>**Access to data and documentation**<br><br>Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential cybersecurity requirements set out in annex I to this law, the market surveillance responsible structure s shall, upon a reasoned request, be granted access, in a language they can easily understand, to the data necessary to assess the design, development, production and vulnerability handling of those | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | including related internal documentation of the relevant economic operator. | | | products, including the internal documentation of the economic operator concerned. | | |
| **A54** | Article 54<br>**Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk**<br><br>1. Where the market surveillance authority of a Member State has sufficient reason to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall, without undue delay and, where appropriate, in cooperation with the relevant CSIRT, 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 with the market surveillance authority as necessary.<br>Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant economic operator to take all appropriate corrective actions to bring the product with digital elements into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period, commensurate with the nature of the cybersecurity risk, as the market surveillance authority may prescribe.<br>The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the corrective actions.<br>2. When determining the significance of a cybersecurity risk referred to in paragraph 1 of this Article, the market surveillance authorities shall also consider non-technical risk factors, in particular those established as a result of Union level coordinated security risk assessments of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555. Where a market surveillance authority 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 competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary. | | **A51** | Article 51<br>**Procedure at national level for products with digital elements presenting a significant cybersecurity risk**<br><br>1. Where the market surveillance responsible structure has sufficient reason to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall immediately, and where appropriate in cooperation with the National CSIRT, assess the product concerned for compliance with all the requirements laid down in this law. The economic operators concerned shall cooperate with the market surveillance responsible structure as necessary.<br>If, during that assessment, the market surveillance responsible structure finds that the product with digital elements does not comply with the requirements laid down in this law, it shall immediately require the economic operator concerned to take all appropriate corrective action to bring the product into compliance with those requirements, or to withdraw or recall the product within a reasonable period, proportionate to the nature of the cybersecurity risk, as determined by the market surveillance responsible structure .<br>The market surveillance responsible structure shall inform the relevant notified body. The legislation in force on market surveillance shall apply to the corrective action.<br>2. When determining the significance of a cybersecurity risk referred to in point 1 of this article, the market surveillance responsible structure s shall also take into account non-technical risk factors, in particular those identified as a result of coordinated national security risk assessments of critical supply chains carried out in accordance with the legislation in force on cybersecurity. Where a market surveillance responsible structure has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk due to non-technical risk factors, it shall inform the national cybersecurity authority and cooperate with it as necessary.<br>3. Upon Albania's accession to the European Union, where the market surveillance responsible structure considers that the non-compliance is not limited to its national territory, it | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 3. 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.<br>4. The economic operator 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.<br>5. Where the economic operator does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict that product with digital elements from being made available on its national market, to withdraw it from that market or to recall it.<br>That authority shall notify the Commission and the other Member States, without delay, of those measures.<br>6. The information referred to in paragraph 5 shall include all available details, in particular the data necessary for the identification of the non-compliant product with digital elements, the origin of 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:<br>(a) a failure of the product with digital elements or of the processes put in place by the manufacturer to meet the essential cybersecurity requirements set out in Annex I;<br>(b) shortcomings in the harmonised standards, European cybersecurity certification schemes or common specifications, as referred to in Article 27.<br>7. 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.<br>8. Where, within three months of receipt of the notification referred to in paragraph 5 of this Article, no objection has been raised by either a Member State or | | | shall inform the Commission and the other Member States of the results of the assessment and of the action it has required the economic operator to take.<br>4. The economic operator shall ensure that appropriate corrective action is taken in respect of all products with digital elements that it has made available on the market in the Republic of Albania.<br>5. Where the economic operator does not take appropriate corrective action within the period referred to in the second subpoint of point 1 of this article, the market surveillance responsible structure shall take all appropriate provisional measures to withdraw the product or restrict its making available on the market, or to ensure that the product is recalled. Upon Albania's accession to the European Union, the market surveillance responsible structure shall immediately inform the Commission and the other Member States of those measures.<br>6. The information referred to in point 5 of this article shall include all available details, in particular the data necessary to identify the non-compliant product with digital elements, its origin, the nature of the alleged non-compliance and the risk involved, the nature and duration of the measures taken, and the arguments put forward by the economic operator concerned. In particular, the market surveillance responsible structure shall indicate whether the non-compliance is due to one or more of the following:<br>a. a failure of the product with digital elements or of the processes put in place by the manufacturer to meet the essential cybersecurity requirements set out in annex I to this law;<br>b. deficiencies in the harmonised standards, cybersecurity certification schemes or common specifications referred to in article 27 of this law.<br>7. Upon Albania"s accession to the European Union, the market surveillance responsible structure shall without delay inform the Commission and the other Member States of any measures adopted and any additional information available concerning the non-compliance of the product with digital elements and, in the event of disagreement with the notified measure, of its objections.<br>8. If, within three months of receipt of the notification referred to in point 5 of this article, no objection has been raised by a Member State or the Commission concerning a provisional measure taken by the market surveillance responsible structure , upon Albania's accession to the European Union that measure shall be deemed justified. This shall be without prejudice to the procedural rights of the economic operator under the legislation in force | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed to be justified. This is without prejudice to the procedural rights of the economic operator concerned in accordance with Article 18 of Regulation (EU) 2019/1020.<br>9. 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 that product from their market, without delay. | | | on market surveillance.<br>9. The market surveillance responsible structure shall ensure that appropriate restrictive measures are taken in respect of the product with digital elements, such as the immediate withdrawal of the product. | | |
| **A55** | Article 55<br>**Union safeguard procedure**<br><br>1. Where, within three months of receipt of the notification referred to in Article 54(5), 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 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 54(5) and notify that decision to the Member State concerned.<br>2. If the national measure is considered to be justified, all Member States shall take the measures necessary to ensure that the non-compliant product with digital elements is withdrawn from their market, and shall inform the Commission accordingly. If the national measure is not considered to be justified, the Member State concerned shall withdraw the measure.<br>3. Where the national measure is considered to be 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 11 of Regulation (EU) No 1025/2012.<br>4. Where the national measure is considered to be 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 27, the Commission shall consider whether to amend or repeal any delegated act adopted pursuant to Article 27(9) that specifies the presumption of conformity concerning that certification scheme.<br>5. Where the national measure is considered to be justified and the non-compliance of the product with digital elements is attributed to shortcomings in common | | | | **N** | Article 55 of the regulation concerns member states and is inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | specifications as referred to in Article 27, the Commission shall consider whether to amend or repeal any implementing act adopted pursuant to Article 27(2) setting out those common specifications. | | | | | |
| **A56** | Article 56<br>**Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk**<br><br>1. Where the Commission has sufficient reason to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk does not comply with the requirements laid down in this Regulation, it shall inform the relevant market surveillance authorities. Where the market surveillance authorities carry out an evaluation of that product with digital elements that may present a significant cybersecurity risk in respect of its compliance with the requirements laid down in this Regulation, the procedures referred to in Articles 54 and 55 shall apply.<br>2. 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, where appropriate, the competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary. The Commission shall also consider the relevance of the identified risks for that product with digital elements in view of its tasks regarding the Union level coordinated security risk assessments of critical supply chains provided for in Article 22 of Directive (EU) 2022/2555, and consult, as necessary, the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and ENISA.<br>3. In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason 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 shall carry out an evaluation of compliance and may request ENISA to provide an analysis to support it. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate with ENISA as necessary. | | | | **N** | Article 56 of the regulation concerns member states and is inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 4. Based on the evaluation referred to in paragraph 3, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To that end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.<br>5. On the basis of the consultation referred to in paragraph 4 of this Article, the Commission may adopt implementing acts to provide for corrective or restrictive measures at Union level, including requiring the products with digital elements concerned to be withdrawn from the market or recalled, 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 62(2).<br>6. The Commission shall immediately communicate the implementing acts referred to in paragraph 5 to the relevant economic operator or operators. Member States shall implement those implementing acts without delay and shall inform the Commission accordingly.<br>7. Paragraphs 3 to 6 shall be applicable for the duration of the exceptional situation that justified the Commission's intervention, provided that the product with digital elements concerned is not brought in compliance with this Regulation. | | | | | |
| **A57** | Article 57<br>**Compliant products with digital elements which present a significant cybersecurity risk**<br><br>1. The market surveillance authority of a Member State shall require an economic operator to take all appropriate measures where, having performed an evaluation under Article 54, it 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 as well as a risk to:<br>(a) the health or safety of persons;<br>(b) the compliance with obligations under Union or national law intended to protect fundamental rights;<br>(c) the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555; or<br>(d) other aspects of public interest protection.<br>The measures referred to in the first subparagraph may include measures to ensure that the product with digital | | **A52** | Article 52<br>**Products with digital elements that comply with the requirements but present a significant cybersecurity risk**<br><br>1. The market surveillance responsible structure shall require an economic operator to take all appropriate measures where, after carrying out an assessment under article 51 of this law, it finds that, although a product with digital elements and the processes put in place by the manufacturer comply with this law, they present a significant cybersecurity risk and a risk to:<br>the health or safety of persons;<br>compliance with obligations under the legislation in force on the protection of fundamental rights;<br>the availability, authenticity, integrity or confidentiality of services provided using an electronic information system by operators of highly critical information infrastructures under the legislation in force on cybersecurity; or<br>ç) other aspects of the protection of the public interest.<br>The measures referred to above may include measures to ensure that the product with digital | **F** | Paragraphs 4 and 5 of Article 57 of the regulation are not applicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 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.<br>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.<br>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.<br>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.<br>5. The Commission shall address the decision referred to in paragraph 4 to the Member States.<br>6. Where the Commission has sufficient reason 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 of this Article, it shall inform and may request the relevant market surveillance authority or authorities to carry out an evaluation and follow the procedures referred to in Article 54 and in paragraphs 1, 2 and 3 of this Article.<br>7. In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason 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 shall carry out an evaluation of the risks presented by that product with digital elements and may request ENISA to | | | elements and the processes put in place by the manufacturer no longer present the relevant risks when made available on the market, the withdrawal or recall of the product, and shall be proportionate to the nature of those risks.<br>2. The manufacturer or other relevant economic operators shall ensure that corrective action is taken in respect of products with digital elements that they have made available on the market in the Republic of Albania within the period set by the market surveillance responsible structure referred to in point 1 of this article.<br>3. Upon Albania's accession to the European Union, the market surveillance responsible structure shall immediately inform the Commission and the other Member States of the measures taken in accordance with point 1 of this article. That information shall include all available details, in particular the data necessary to identify the products with digital elements, their origin and supply chain, the nature of the risk involved, and the nature and duration of the measures taken.<br>4. Where the responsible ministry has sufficient reason to consider, including on the basis of information provided by the National Cyber Security Authority, that a product with digital elements, despite complying with this law, presents the risks referred to in point 1 of this article, it shall inform the competent authority and may request that the authority or the market surveillance responsible structure s carry out an assessment and follow the procedures referred to in article 51 and points 1, 2 and 3 of this article.<br>5. In circumstances justifying immediate intervention to preserve the proper functioning of the internal market, and where the responsible ministry has sufficient reason to consider that the product with digital elements referred to in point 4 of this article continues to present the risks referred to in point 1 and that the market surveillance responsible structure s have not taken effective measures, the responsible ministry shall assess the risks presented by the product and may request the National Cyber Security Authority to carry out an analysis supporting that assessment, and shall inform the market surveillance responsible structure s accordingly. The economic operators concerned shall cooperate with the National Cyber Security Authority as necessary.<br>6. On the basis of the assessment referred to in point 5 of this article, the responsible ministry may determine whether a corrective or restrictive measure at national level is necessary. For that purpose, it shall immediately consult the economic | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | provide an analysis to support that evaluation and shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate with ENISA as necessary.<br>8. Based on the evaluation referred to in paragraph 7, the Commission may establish that a corrective or restrictive measure is necessary at Union level. To that end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.<br>9. On the basis of the consultation referred to in paragraph 8 of this Article, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including requiring the products with digital elements concerned to be withdrawn from the market, or recalled, 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 62(2).<br>10. The Commission shall immediately communicate the implementing acts referred to in paragraph 9 to the relevant economic operator or operators. Member States shall implement those implementing acts without delay and shall inform the Commission accordingly.<br>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 product with digital elements concerned continues to present the risks referred to in paragraph 1. | | | operator or operators concerned.<br>7. On the basis of the consultation referred to in point 6 of this article, the Council of Ministers shall, on a proposal from the minister responsible for electronic and digital communications, approve corrective or restrictive measures at national level in accordance with relevant European Union practice, including a requirement that the products with digital elements be withdrawn from the market or from being made available on the market within a reasonable period proportionate to the nature of the risk.<br>8. The responsible ministry shall immediately notify the economic operator or operators concerned of the decisions of the Council of Ministers referred to in point 7 of this article. The economic operators shall implement those decisions immediately and inform the responsible ministry accordingly.<br>9. Points 4 to 8 of this article shall apply for the duration of the emergency situation justifying the intervention of the responsible ministry, for as long as the product with digital elements continues to present the risks referred to in point 1 of this article. | | |
| **A58** | Article 58<br>**Formal non-compliance**<br><br>1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant manufacturer to put an end to the non-compliance concerned:<br>(a) the CE marking has been affixed in violation of Articles 29 and 30;<br>(b) the CE marking has not been affixed;<br>(c) the EU declaration of conformity has not been drawn up;<br>(d) the EU declaration of conformity has not been drawn up correctly;<br>(e) the identification number of the notified body which is involved in the conformity assessment procedure, where applicable, has not been affixed;<br>(f) the technical documentation is either not available or not complete. | | **A53** | Article 53<br>**Formal non-compliance**<br><br>1. Where the market surveillance responsible structure makes any of the following findings, it shall require the manufacturer concerned to put an end to the non-compliance concerning:<br>a. the CE marking having been affixed in breach of articles 29 and 30 of this law;<br>b. the CE marking not having been affixed;<br>c. the EU declaration of conformity not having been drawn up;<br>ç. the EU declaration of conformity having been drawn up incorrectly;<br>d. the identification number of the notified body involved in the conformity assessment procedure, where applicable, not having been affixed;<br>dh. the technical documentation being unavailable or incomplete. | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 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 point 1 of this article persists, the market surveillance responsible structure shall take all appropriate measures to restrict or withdraw the product with digital elements from being made available on the market, or to ensure that it is recalled or withdrawn from the market. | | |
| **A59** | Article 59<br>**Joint activities of market surveillance authorities**<br><br>1. Market surveillance authorities may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and the 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.<br>2. The Commission or ENISA shall propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products with digital elements that fall within the scope of this Regulation with the requirements laid down in this Regulation.<br>3. The market surveillance authorities and, 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.<br>4. A market surveillance authority may use any information obtained as a result of the joint activities carried out as part of any investigation that it undertakes.<br>5. The market surveillance authority concerned and, where applicable, the Commission, shall make the agreement on joint activities, including the names of the parties involved, available to the public. | | **A54** | Article 54<br>**Joint activities of market surveillance authorities**<br><br>1. The market surveillance responsible structure s may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and protecting consumers in relation to specific products with digital elements placed or made available on the market, in particular products with digital elements frequently found to present cybersecurity risks.<br>2. The market surveillance responsible structure and, where applicable, the responsible ministry shall ensure that agreements on joint activities do not result in unfair competition between economic operators and do not adversely affect the objectivity, independence or impartiality of the parties to the agreement.<br>3. The market surveillance responsible structure may use any information obtained as a result of joint activities in any verification it carries out.<br>4. The market surveillance responsible structure and, where applicable, the responsible ministry shall make public the agreement on joint activities, including the names of the parties involved. | **F** | Point 2 of Article 59 of the CRA Regulation is inapplicable in the case of Albania, as it relates to obligations of the Commission and ENISA. |
| **A60** | Article 60<br>**Sweeps**<br><br>1. Market surveillance authorities shall 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. Those sweeps may include inspections of products with digital elements acquired under a cover identity. | | **A55** | **Article 55**<br>**Sweep**<br><br>1. The market surveillance responsible structure s shall carry out coordinated, simultaneous control actions on specific products with digital elements or categories thereof to check compliance or detect infringements of this law. Such actions may also include inspections of products with digital elements obtained under a covert identity.<br>2. Unless otherwise agreed by the market surveillance responsible structure s involved, the | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 2. Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep shall, where appropriate, make the aggregated results publicly available.<br>3. Where, in the performance of its tasks, including based on the notifications received pursuant to Article 14(1) and (3), ENISA identifies categories of products with digital elements for which sweeps may be organised, it shall submit a proposal for a sweep to the coordinator referred to in paragraph 2 of this Article for the consideration of the market surveillance authorities.<br>4. When conducting sweeps, the market surveillance authorities involved may use the investigation powers set out in Articles 52 to 58 and any other powers conferred upon them by national law.<br>5. Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps. | | | control actions shall be coordinated by the responsible ministry. Where appropriate, the coordinator of the control actions shall make the results collected publicly available.<br>3. Where, in the performance of its tasks, including on the basis of notifications received in accordance with points 1) and 3) of article 14 of this law, the National Cyber Security Authority identifies categories of products with digital elements for which control actions may be organised, it shall submit a proposal for a control action to the coordinator referred to in point 2 of this article for consideration by the market surveillance authorities.<br>4. When carrying out control actions, the market surveillance responsible structure s involved may use the verification powers set out in articles 49 to 53 of this law and any other powers conferred on them by other legislation in force.<br>5. The market surveillance responsible structure s may invite officials and other persons accompanying them who are authorised by the responsible ministry to participate in control actions. | | |
| **A61** | Article 61<br>**Exercise of the delegation**<br><br>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.<br>2. The power to adopt delegated acts referred to in Article 2(5), second subparagraph, Article 7(3), Article 8(1) and (2), Article 13(8), fourth subparagraph, Article 14(9), Article 25, Article 27(9), Article 28(5) and Article 31(5) shall be conferred on the Commission for a period of five years from 10 December 2024. 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.<br>3. The delegation of power referred to in Article 2(5), second subparagraph, Article 7(3), Article 8(1) and (2), Article 13(8), fourth subparagraph, Article 14(9), Article 25, Article 27(9), Article 28(5) and Article 31(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 | | | | **N** | Article 61 of the regulation concerns member states and is inapplicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.<br>4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.<br>5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.<br>6. A delegated act adopted pursuant to Article 2(5), second subparagraph, Article 7(3), Article 8(1) or (2), Article 13(8), fourth subparagraph, Article 14(9), Article 25, Article 27(9), Article 28(5) or Article 31(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council. | | | | | |
| **A62** | Article 62<br>**Committee procedure**<br><br>1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.<br>2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.<br>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. | | | | **N** | Article 62 of the regulation concerns member states and is inapplicable. |
| **A63** | Article 63<br>**Confidentiality**<br><br>1. All parties involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:<br>(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 (EU) 2016/943 of the European Parliament and of the Council (37); | | **A56** | Article 56<br>**Confidentiality**<br><br>1. All parties involved in the implementation of this law shall respect the confidentiality of information and data obtained in carrying out their tasks and activities, in order to protect, in particular:<br>a. intellectual property rights and confidential business information or trade secrets of a natural or legal person, including source code, except as provided for in the legislation in force;<br>b. the effective implementation of this law, in particular for the purposes of inspections, verifications or audits; | **F** | Paragraph 4 of Article 63 of the regulation concerns the EC and the Member States and, as such, is not applicable. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | (b) the effective implementation of this Regulation, in particular for the purposes of inspections, investigations or audits;<br>(c) public and national security interests;<br>(d) integrity of criminal or administrative proceedings.<br>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.<br>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.<br>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. | | | c. public and national security interests;<br>ç. the integrity of criminal or administrative proceedings.<br>2. Without prejudice to point 1 of this article, information exchanged on a confidential basis between the market surveillance responsible structure s and the responsible ministry and, upon Albania's accession to the European Union, between the market surveillance responsible structure of the Republic of Albania and the market surveillance responsible structure s of other countries and the European Commission, shall not be disclosed without the prior consent of the originating market surveillance responsible structure .<br>3. Points 1 and 2 of this article shall not affect the rights and obligations of the responsible ministry and notified bodies concerning the exchange of information and dissemination of warnings, or the obligations of persons to provide information under the legislation in force on criminal matters. | | |
| **A64** | Article 64<br>**Penalties**<br><br>1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, without delay, notify the Commission of those rules and measures and shall notify it, without delay, of any subsequent amendment affecting them.<br>2. Non-compliance with the essential cybersecurity requirements set out in Annex I and the obligations set out in Articles 13 and 14 shall be subject to administrative fines of up to EUR 15 000 000 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.<br>3. Non-compliance with the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4),<br>Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual | | **A57** | Article 57<br>**Administrative offences and penalties**<br><br>1. Failure to comply with the essential cybersecurity requirements set out in annex I to this law and the obligations laid down in articles 13 and 14 of this law shall be punishable by an administrative fine of up to ALL 15 000 000 or, where the offender is a company, up to 2.5 % of its total annual turnover for the preceding financial year, whichever is higher.<br>2. Failure to comply with the obligations laid down in articles 18 to 23, article 28, point 1 to 4 of article 30, points 1 to 4 of article 31, points 1, 2 and 3 of article 32, point 4 of article 33, and articles 39, 41, 45, 47 and 50 shall be punishable by an administrative fine of up to ALL 10 000 000 or, where the offender is an undertaking, up to 2 % of its total annual turnover for the preceding financial year, whichever is higher.<br>3. Providing inaccurate, incomplete or misleading information to notified bodies and market surveillance responsible structure s in response to a request shall be punishable by an administrative fine of up to ALL 5 000 000 or, where the offender is a company, up to 1 % of its total annual turnover for the preceding financial year, whichever is higher.<br>4. When deciding on the amount of the administrative | **F** | Paragraphs 1, 6, and 8 of Article 64 of the regulation concern Member States and, as such, do not apply. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | turnover for the preceding financial year, whichever is higher.<br>4. 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 EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.<br>5. 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:<br>(a) the nature, gravity and duration of the infringement and of its consequences;<br>(b) whether administrative fines have been already applied by the same or other market surveillance authorities to the same economic operator for a similar infringement;<br>(c) the size, in particular with regard to microenterprises and small and medium sized-enterprises, including start-ups, and the market share of the economic operator committing the infringement.<br>6. Market surveillance authorities that apply administrative fines shall communicate that application 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.<br>7. Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and public bodies established in that Member State.<br>8. 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.<br>9. 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.<br>10. By way of derogation from paragraphs 3 to 9, the administrative fines referred to in those paragraphs shall not apply to the following:<br>(a) manufacturers that qualify as microenterprises or small enterprises with regard to any | | | fine in each individual case, all relevant circumstances of the specific situation shall be taken into account, with particular consideration given to the following:<br>a. the nature, gravity and duration of the infringement and its consequences;<br>b. whether administrative fines have already been imposed by the same or other market surveillance responsible structure s on the same economic operator for a similar infringement;<br>c. the size of the economic operator responsible for the infringement, in particular whether it is a microenterprise or a small or medium-sized enterprise, including a start-up, and its market share.<br>5. The Council of Ministers, upon the proposal of the Minister responsible for electronic and digital communications, as well as the economy and innovation, shall lay down the rules concerning the cases and the amounts of administrative fines to be imposed on public authorities and public bodies established in the Republic of Albania.<br>6. Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measure applied by the market surveillance responsible structure s for the same infringement.<br>7. By way of derogation from points 2 to 6 of this article, the administrative fines referred to in those points shall not apply to:<br>a. manufacturers qualifying as microenterprises or small enterprises in relation to any failure to meet the deadline referred to in letter a) of point 2 of article 14 or letter a) of point 4 of Article 14 of this law;<br>b. any infringement of this law by open-source software stewards. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | failure to meet the deadline referred to in Article 14(2), point (a), or Article 14(4), point (a);<br>(b) any infringement of this Regulation by open-source software stewards. | | | | | |
| **A65** | Article 65<br>**Representative actions**<br><br>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. | | | | **N** | Article 65 of the regulation concerns member states and is inapplicable. |
| **A66** | Article 66<br>**Amendment to Regulation (EU) 2019/1020**<br><br>In Annex I to Regulation (EU) 2019/1020, the following point is added:<br><br>‘72. Regulation (EU) 2024/2847 of the European Parliament and of the Council (*). | | | | **N** | Article 66 of the regulation concerns the EC and is inapplicable. |
| **A67** | Article 67<br>**Amendment to Directive (EU) 2020/1828**<br><br>In Annex I to Directive (EU) 2020/1828, the following point is added:<br>‘69. Regulation (EU) 2024/2847 of the European Parliament and of the Council (*). | | | | **N** | Article 67 of the regulation concerns the EC and is inapplicable. |
| **A68** | Article 68<br>**Amendment to Regulation (EU) No 168/2013**<br><br>In Part C1, in the table, of Annex II to Regulation (EU) No 168/2013 of the European Parliament and of the Council (38), the following entry is added:<br>‘<br><br>16 18 protection of vehicle against cyberattacks x x<br>x x x x<br>x x x x<br>x x x x | | | | **N** | Article 68 of the regulation concerns the EC and is inapplicable. |
| **A69** | Article 69<br>**Transitional provisions**<br><br>1. EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for products with digital elements that are subject to Union harmonisation legislation other than this Regulation shall remain valid until 11 June 2028, unless they expire before that date, or unless otherwise specified in such other Union harmonisation legislation, | | **A59** | Article 59<br>**Transitional provisions**<br><br>1. EU-type examination certificates and approval decisions issued in relation to cybersecurity requirements under the European Union legislation in force, other than this law, for products with digital elements shall remain valid until 31 December 2029, unless they expire before that date or unless otherwise specified in other legislation in force, in which case they shall remain | **F** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | in which case they shall remain valid as referred to in that legislation.<br>2. Products with digital elements that have been placed on the market before 11 December 2027 shall be subject to the requirements set out in this Regulation only if, from that date, those products are subject to a substantial modification.<br>3. By way of derogation from paragraph 2 of this Article, the obligations laid down in Article 14 shall apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027. | | | valid as provided for in the relevant legislation.<br>2. Products with digital elements placed on the market before the entry into force of this law shall be subject to the requirements laid down in this law only if, from that date, those products undergo a substantial modification.<br>3. By way of derogation from point 2 of this article, the obligations laid down in article 14 of this law shall apply to all products with digital elements falling within the scope of this law that were placed on the market before its entry into force. | | |
| **A70** | Article 70<br>**Evaluation and review**<br><br>1. By 11 December 2030 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. Those reports shall be made public.<br>2. By 11 September 2028, the Commission shall, after consulting ENISA and the CSIRTs network, submit a report to the European Parliament and to the Council, assessing the effectiveness of the single reporting platform set out in Article 16, as well as the impact of the application of the cybersecurity-related grounds referred to Article 16(2) by the CSIRTs designated as coordinators on the effectiveness of the single reporting platform as regards the timely dissemination of received notifications to other relevant CSIRTs. | | **A60** | **Article 60**<br>**Assessment and review**<br><br>1. The responsible ministry shall draw up a report on the assessment and review of this law. Those reports shall be made public. | **F** | |
| **A71** | Article 71<br>**Entry into force and application**<br><br>1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.<br>2. This Regulation shall apply from 11 December 2027.<br>However, Article 14 shall apply from 11 September 2026 and Chapter IV (Articles 35 to 51) shall apply from 11 June 2026.<br><br>This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at Strasbourg, 23 October 2024.<br>For the European Parliament The President<br>R. METSOLA For the Council The President<br>ZSIGMOND B. P. | | | | **N** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Annex I** | **ANNEX I**<br>**ESSENTIAL CYBERSECURITY REQUIREMENTS** | | **Annex I** | **ANNEX I**<br>**ESSENTIAL CYBERSECURITY REQUIREMENTS** | **F** | |
| **Annex I**<br>**Part I** | Part I<br>Cybersecurity requirements relating to the properties of products with digital elements | | **Annex I**<br>**Part I** | Part I<br>Cybersecurity requirements relating to the properties of products with digital elements | **F** | |
| **Annex I**<br>**Part II** | Part II<br>Vulnerability handling requirements | | **Annex I**<br>**Part II** | Part II<br>Vulnerability-handling requirements | **F** | |
| **Annex II** | **ANNEX II**<br>**INFORMATION AND INSTRUCTIONS TO THE USER** | | **Annex II** | **ANNEX II**<br>**USER INFORMATION AND INSTRUCTIONS** | **F** | |
| **Annex III**<br>**Class I** | **ANNEX III**<br>**IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS**<br>Class I | | **Annex III**<br>**Class I** | **ANNEX III**<br>**IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS**<br>Class I | **F** | |
| **Annex III**<br>**Class II** | **ANNEX III**<br>**IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS**<br>Class II | | **Annex III**<br>**Class II** | **ANNEX III**<br>**IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS**<br>Class II | **F** | |
| **Annex IV** | **ANNEX IV**<br>**CRITICAL PRODUCTS WITH DIGITAL ELEMENTS** | | **Annex IV** | **ANNEX IV**<br>**CRITICAL PRODUCTS WITH DIGITAL ELEMENTS** | **F** | |
| **Annex V** | **ANNEX V**<br>**EU DECLARATION OF CONFORMITY** | | **Annex V** | **ANNEX V**<br>**EU DECLARATION OF CONFORMITY** | **F** | |
| **Annex VI** | **ANNEX VI**<br>**SIMPLIFIED EU DECLARATION OF CONFORMITY** | | **Annex VI** | **ANNEX VI**<br>**SIMPLIFIED EU DECLARATION OF CONFORMITY** | | |
| **Annex VII** | **ANNEX VII**<br>**CONTENT OF THE TECHNICAL DOCUMENTATION** | | **Annex VII** | **ANNEX VII**<br>**CONTENT OF THE TECHNICAL DOCUMENTATION** | | |
| **Annex VIII** | **ANNEX VIII**<br>**CONFORMITY ASSESSMENT PROCEDURES** | | **Annex VIII** | **ANNEX VIII**<br>**CONFORMITY ASSESSMENT PROCEDURES** | | |
| **Annex VIII**<br>**Part I** | Part I<br>Conformity assessment procedure based on internal control (based on module A) | | **Annex VIII**<br>**Part I** | Part I<br>Conformity assessment procedure based on internal control (based on Module A) | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Annex VIII Part II** | Part II<br>EU-type examination (based on module B) | | **Annex VIII Part II** | Part II<br>EU-type examination (based on Module B) | | |
| **Annex VIII Part III** | Part III<br>Conformity to type based on internal production control (based Module C) | | **Annex VIII Part III** | Part III<br>Conformity to type based on internal production control (based on module C) | | |
| **Annex VIII Part IV** | Part IV<br>Conformity based on full quality assurance (based on module H) | | **Annex VIII Part IV** | Part IV<br>Conformity based on full quality assurance (based on Module H) | | |
| | | | | | | |