REPUBLIC OF ALBANIA

Parliament

D R A F T L A W

No._____/2026

ON CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS AND CYBER RESILIENCE

Pursuant to articles 78, 81, point 1, and 83, point 1, of the Constitution, upon the proposal of the Council of Ministers, the Parliament of the Republic of Albania

D E C I D E S:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This law lays down:

a) rules for placing products with digital elements on the market, in order to ensure the cybersecurity of those products;
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;
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;
ç) rules on market surveillance, including monitoring and enforcement of the requirements laid down in this article.

Article 2

Scope

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.
2. This law shall not apply to products with digital elements regulated by the legislation in force as follows:
a) medical devices pursuant to law no. 89/2014 “On Medical Devices’;

b) *in vitro* medical devices pursuant to law no. 89/2014 “On Medical Devices’;
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.
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.
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.
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:
a) such a restriction or exclusion is consistent with the overall regulatory framework applicable to those products; and
b) the sectoral rules achieve the same or a higher level of protection than this law.
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.
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.
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.
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.

Article 3

Definitions

For the purposes of this law, the following definitions shall apply:

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.
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.
3. “Cybersecurity” has the same meaning as in law No. 25/2024 “On Cybersecurity”.
4. “Software” means the part of an electronic information system consisting of computer code.
5. “Hardware” means a physical electronic information system or parts thereof capable of processing, storing or transmitting digital data.
6. “Component” means software or hardware intended to be integrated into an electronic information system.
7. “Electronic information system” means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data.

8. “Logical connection” means a virtual representation of a data connection implemented through a software interface.
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.
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.
11. “Endpoint” means any device connected to a network that serves as an entry point to that network.
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.
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.
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.
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.
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.
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.
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.
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”.
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.
21. “Placing on the market” means the first making available of a product with digital elements on the market.
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.
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.
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.

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.
26. “Notifying authority” means the national authority responsible for establishing and carrying out the procedures necessary for the assessment, designation and notification of conformity assessment bodies and for monitoring them.
27. “Conformity assessment” means the process of verifying whether the essential cybersecurity requirements set out in annex I to this law have been fulfilled.
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.
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.
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.
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.
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.
33. “Market surveillance responsible structure” means the authority responsible for market surveillance as specified in the legislation in force on market surveillance.
34. “International standard” has the same meaning as in law No. 9870/2008 “On Standardisation”, as amended.
35. “European standard” has the same meaning as in law No. 9870/2008 “On Standardisation”, as amended.
36. “Harmonised standard” has the same meaning as in law No. 9870/2008 “On Standardisation”, as amended.
37. “Cybersecurity risk” has the same meaning as in law No. 25/2024 “On Cybersecurity”.
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.
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.
40. “Vulnerability” has the same meaning as in law No. 25/2024 “On Cybersecurity”.
41. “Exploitable vulnerability” means a vulnerability that has the potential to be effectively used by a malicious actor under practical operational conditions.
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.
43. “Incident” has the same meaning as in law No. 25/2024 “On Cybersecurity”.
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.
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.
46. “Cyber threat” has the same meaning as in law No. 25/2024 “On Cybersecurity”.
47. “Personal data” has the same meaning as in law No. 124/2024 “On the Protection of Personal Data”.
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.
49. “Recall” means any measure aimed at achieving the return of a product that has already been made available to the end user.
50. “Withdrawal” means any measure aimed at preventing a product in the supply chain from being made available on the market.
51. “CSIRT designated as coordinator” means the National CSIRT under law No. 25/2024 “On Cybersecurity”.

Article 4

Free movement

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.
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.
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.
4. Point 3 of this article shall not apply to safety components provided for in national legislation other than this law.

Article 5

Procurement or use of products with digital elements

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.
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.

Article 6

Requirements for products with digital elements

Products with digital elements shall be made available on the market only where:

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
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.

Article 7

Important products with digital elements

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.
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:

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;
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.

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.
4. Where necessary, on a proposal from the minister responsible for electronic and digital communications, the Council of Ministers shall, in 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.

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.

Article 8

Critical products with digital elements

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.

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".

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 authorities and the market to implement the relevant certification scheme.

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.

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.

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.

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:

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;
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.

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.

Article 9

Consultation of interested parties

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-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:

a) when preparing the guidance referred to in article 26 of this law;
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;
c) when carrying out preparatory work for the assessment and review of this law.

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.

Article 10

Enhancing skills in a cyber digital environment

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:

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 responsible structures and conformity assessment bodies;
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.

Article 11

General product safety

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.

Article 12

High-risk AI systems

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:

a) they meet the essential cybersecurity requirements set out in part I of annex I to this law;
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
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.

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 notification procedure under the legislation in force on artificial intelligence.

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.

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.

CHAPTER II

OBLIGATIONS OF ECONOMIC OPERATORS AND PROVISIONS RELATING TO FREE AND OPEN-SOURCE SOFTWARE

Article 13

Obligations of manufacturers

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.

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.
3. The cybersecurity risk assessment shall be documented and updated as necessary during the support period determined in accordance with point 8 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.
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.
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.
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 relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.
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.
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.
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.
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.
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.

Manufacturers shall include the information taken into account when determining the support period of a product with digital elements in the technical documentation referred to in annex VII to this law.
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.
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.
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.
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.
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.
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.
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.
13. Manufacturers shall keep the technical documentation and the EU declaration of conformity available to the market surveillance responsible structures 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.
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.

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.
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 responsible structures.
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.
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.
The single point of contact shall enable users to choose their preferred means of communication and shall not limit those means to automated tools.
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 responsible structures. 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 responsible structures 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.
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.
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.
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.
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.
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.
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.
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.

Article 14

Reporting obligations of manufacturers

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 16 of this Law, upon accession to the European Union.
2. For the purposes of the notification referred to in paragraph 1 of this Article, the manufacturer shall submit:
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;
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;
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:
i. a description of the vulnerability, including its severity and impact;
ii. where available, information relating to any malicious actor that has exploited or is exploiting the vulnerability;
iii. details of the security update or other corrective measures made available to remedy the vulnerability.
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.

4. For the purposes of the notification referred to in paragraph 3 of this Article, the manufacturer shall submit:
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;
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;
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:
i. a detailed description of the incident, including its severity and impact;
ii. the type of threat or root cause that is likely to have triggered the incident;
iii. the mitigating measures implemented and those that are ongoing.
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:
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
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.
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.
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.
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.
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.
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.

Article 15

Voluntary reporting

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.
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.
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.
The National CSIRT may give priority to the processing of mandatory notifications over voluntary notifications.
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, the National CSIRT shall inform the manufacturer immediately.
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.

Article 16

Establishment of the single reporting platform

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.
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.
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.
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 accordance with the procedure laid down in this paragraph.
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:

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;
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
c) the reported vulnerability poses an imminent high cybersecurity risk arising from further dissemination;
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.
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.
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.
This requirement shall not prevent manufacturers from voluntarily reporting a vulnerability in accordance with the procedure laid down in this Article.

Article 17
Other reporting provisions

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.
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.
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.
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".
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.

Article 18

Authorised representatives

1. A manufacturer may appoint an authorised representative by written mandate.
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.
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 responsible structures. The mandate shall allow the authorised representative to do at least the following:
   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;
   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;
   c) to cooperate with the market surveillance responsible structures, at their request, on any action taken to eliminate risks posed by a product with digital elements covered by the authorised representative's mandate.

Article 19

Obligations of importers

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.
2. Before placing a product with digital elements on the market, importers shall ensure that:
   a) the appropriate conformity assessment procedures referred to in article 32 of this law have been carried out by the manufacturer;
   b) the manufacturer has drawn up the technical documentation;
   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 responsible structures;
   (ç) the manufacturer has complied with the requirements laid down in points 15, 16 and 19 of article 13 of this law.

For the purposes of this point, importers shall be able to provide the necessary documents demonstrating compliance with the requirements laid down in this article.
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.

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.

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 responsible structures.

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.

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.

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.

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.

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.

Article 20

Obligations of distributors

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.

2. Before making a product with digital elements available on the market, distributors shall verify that:

a) the product with digital elements bears the CE marking;

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.

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.

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.

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 responsible structures, providing details, in particular, of the non-compliance and any corrective measures taken.

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.

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 situation and, by any available means and to the extent possible, users of the products with digital elements placed on the market.

Article 21

Cases in which the obligations of manufacturers apply to importers and distributors

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.

Article 22

Other cases in which the obligations of manufacturers apply

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.

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.

Article 23

Identification of economic operators

1. Upon request, economic operators shall provide the market surveillance responsible structure s with the following information:
   a) the name and address of any economic operator that supplied them with a product with digital elements;
   b) where available, the name and address of any economic operator to whom they supplied a product with digital elements.
2. Economic operators shall be able to present the information referred to in point 1 of this 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.

Article 24

Obligations of open-source software stewards

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.
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.
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.

Article 25
Attestation of security of free and open-source software

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.

Article 26

Guidance

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.
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:
   a) the scope of this law, with particular emphasis on remote data processing solutions and free and open-source software;
   b) the application of support periods to specific categories of products with digital elements;
   c) guidance for manufacturers subject to this law who are also subject to other relevant legislation in force;
   (ç) the concept of substantial modification.
3. When preparing the guidance under this article, the responsible minister shall consult the relevant interested parties.

CHAPTER III

CONFORMITY OF PRODUCTS WITH DIGITAL ELEMENTS

Article 27

Presumption of conformity

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.
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.
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.

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.
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.
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 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.

Article 28

EU declaration of conformity

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.
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.
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.
4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the conformity of the product with digital elements.
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 account of technological developments in accordance with relevant European Union practice.

Article 29

General principles of the CE marking

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.

Article 30

Rules and conditions for affixing the CE marking

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.
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.
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.
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.
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.
5. The affixing of the CE marking to products with digital elements shall build on existing 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.
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.

Article 31

Technical documentation

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.

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.

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.
4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in Albanian.
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, 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.

Article 32

Conformity assessment procedures for products with digital elements

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:
   a) the internal control procedure (based on Module A) set out in annex VIII to this law;
   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;
   c) the conformity assessment based on full quality assurance (based on Module H) set out in annex VIII to this law; or
   ç) where available and applicable, a cybersecurity certification scheme in accordance with point 9 of article 27 of this law.
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:
   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;
   b) a conformity assessment based on full quality assurance (based on Module H) set out in annex VIII to this law.
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:
   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;

b) a conformity assessment based on full quality assurance (based on Module H) set out in annex VIII to this law;
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.

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:

a) a cybersecurity certification scheme in accordance with point 1 of article 8 of this law;
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.

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.

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.

Article 33

Support measures for microenterprises and small and medium-sized enterprises, including start-ups

1. Where appropriate, the ministry responsible for the economy shall take the following actions, tailored to the needs of microenterprises and small enterprises:

a) organise specific awareness-raising and training activities on the implementation of this law;
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;
c) support testing and conformity assessment activities, including, where necessary, with the support of the European Cybersecurity Competence Centre.

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.

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.

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 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.

Article 34

Mutual recognition agreements

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.

CHAPTER IV

NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

Article 35

Notification

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.

Article 36

Notifying authorities

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, designation and notification of conformity assessment bodies, as well as for monitoring them, including compliance with article 41 of this law.

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.

3. The Notifying Authority shall retain full responsibility for the tasks performed by the body referred to in point 2 of this article.

Article 37

Requirements for notifying authorities

1. The notifying authority shall be established in such a way as to avoid any conflict of interest with conformity assessment bodies.
2. The notifying authority shall be organised and operated so as to safeguard the objectivity and impartiality of its activities.

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.
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.
5. The notifying authority shall safeguard the confidentiality of the information it receives.
6. The notifying authority shall have a sufficient number of competent personnel available for the proper performance of its tasks.

Article 38

Information obligation of the notifying authority

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 39

Requirements for notified bodies

1. For the purposes of notification, a conformity assessment body shall meet the requirements laid down in points 2 to 12 of this article.
2. A conformity assessment body shall be established under the legislation in force on accreditation and shall be a legal person.
3. A conformity assessment body shall be an independent third-party body from the organisation or product with digital elements that it assesses.
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.
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.

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.

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.
5. Conformity assessment bodies and their personnel shall carry out conformity assessment activities with the highest degree of professional 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.
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.
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:

a) personnel with sufficient and appropriate technical knowledge and experience to carry out the conformity assessment tasks;
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;
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.

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.
7. The personnel responsible for carrying out conformity assessment activities shall have:

a) technical and vocational training covering all conformity assessment activities in respect of which the conformity assessment body is notified;
b) satisfactory knowledge of the requirements of the assessments they carry out and appropriate authority to carry out those assessments;
c) appropriate knowledge and understanding of the essential cybersecurity requirements set out in annex I to this law, the applicable harmonised standards and common specifications, and the relevant provisions of other legislation in force and secondary legislation;
ç) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

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.

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.
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 responsible structures, while intellectual property rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this point.

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.
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.

Article 40

Presumption of conformity of notified bodies

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 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.

Article 41

Subsidiaries and subcontracting by notified bodies

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.
2. Notified bodies shall assume full responsibility for the tasks performed by subcontractors or subsidiaries, wherever they are established.
3. Activities may be subcontracted or carried out by a subsidiary only with the manufacturer"s agreement.
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.

Article 42

Application for notification

1. A conformity assessment body shall submit an application for notification to the notifying authority.
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.
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.

Article 43

Notification procedure

1. The notifying authority shall notify only conformity assessment bodies that have fulfilled the requirements laid down in article 39 of this law.
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.
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.
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.
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.
Only such a body shall be considered a notified body for the purposes of this law.
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.

Article 44

Changes to notifications

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.
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.

Article 45

Operational obligations of notified bodies

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.
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.
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.
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.
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.
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.

Article 46

Appeals against decisions of notified bodies

The legislation in force shall ensure that an appeal procedure is available against decisions of notified bodies.

Article 47

Information obligation of notified bodies

1. Notified bodies shall inform the notifying authority of the following:

   a) any refusal, restriction, suspension or withdrawal of a certificate;
   b) any circumstance affecting the scope or conditions of notification;
   c) any request for information received from the market surveillance responsible structure concerning conformity assessment activities;
   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.

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.

Article 48

Coordination of notified bodies

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.
2. The notifying authority shall ensure that notified bodies participate in the group"s work, either directly or through designated representatives.

CHAPTER V

MARKET SURVEILLANCE AND ENFORCEMENT

Article 49

Market surveillance and control of products with digital elements on the internal market

1. The legislation in force on market surveillance shall apply to products with digital elements falling within the scope of this law.
2. The market surveillance responsible structure s shall ensure the effective enforcement of this law.
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.
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.
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.
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.
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 where that guidance or advice concerns the processing of personal data.
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.
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.
9. The ministry responsible for the relevant field shall encourage and facilitate the exchange of experience between the market surveillance rsponsible structures.
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.
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.
12. Where necessary, the market surveillance responsible structure s shall facilitate cooperation with interested parties, including scientific, research and consumer organisations.
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.
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.
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.

Article 50

Access to data and documentation

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 products, including the internal documentation of the economic operator concerned.

Article 51

Procedure at national level for products with digital elements presenting a significant cybersecurity risk

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.

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 .

The market surveillance responsible structure shall inform the relevant notified body. The legislation in force on market surveillance shall apply to the corrective action.

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.

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 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.

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.

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.

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:

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;
b) deficiencies in the harmonised standards, cybersecurity certification schemes or common specifications referred to in article 27 of this law.

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.
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 on market surveillance.
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.

Article 52

Products with digital elements that comply with the requirements but present a significant cybersecurity risk

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:

a) the health or safety of persons;
b) compliance with obligations under the legislation in force on the protection of fundamental rights;
c) 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
ç) other aspects of the protection of the public interest.

The measures referred to above may include measures to ensure that the product with digital 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.
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.
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.
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.

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.
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 operator or operators concerned.
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.
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.
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.

Article 53

Formal non-compliance

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:

a) the CE marking having been affixed in breach of articles 29 and 30 of this law;
b) the CE marking not having been affixed;
c) the EU declaration of conformity not having been drawn up;
ç) the EU declaration of conformity having been drawn up incorrectly;
d) the identification number of the notified body involved in the conformity assessment procedure, where applicable, not having been affixed;
dh) the technical documentation being unavailable or incomplete.

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.

Article 54

Joint activities of market surveillance responsible structures

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.
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.
3. The market surveillance responsible structure may use any information obtained as a result of joint activities in any verification it carries out.
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.

Article 55

Sweep

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.
2. Unless otherwise agreed by the market surveillance responsible structure s involved, the control actions shall be coordinated by the responsible ministry. Where appropriate, the coordinator of the control actions shall make the results collected publicly available.
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 responsible structures.
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.
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.

CHAPTER VI

CONFIDENTIALITY AND PENALTIES

Article 56

Confidentiality

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:

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;
b) the effective implementation of this law, in particular for the purposes of inspections, verifications or audits;
c) public and national security interests;
ç) the integrity of criminal or administrative proceedings.

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 .

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.

Article 57

Administrative offences and penalties

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.

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.

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.

4. 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, with particular consideration given to the following:
a) the nature, gravity and duration of the infringement and its consequences;
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;
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.

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.

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.
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:

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;
b) any infringement of this law by open-source software stewards.

CHAPTER VII

TRANSITIONAL AND FINAL PROVISIONS

Article 58

Secondary legislation

1. The Council of Ministers shall adopt, within 24 months from the entry into force of this Law, the by-laws implementing Articles 7, points 3, 4 and 5; 8, points 1 and 4; 13, points 8 and 24; 14, point 9; 25; 27, points 1, 2 and 5; 28, point 5; 30, point 6; 31, point 5; 33, point 4; 36, point 1; 52, point 7; and 57, point 5.

2. The minister responsible for the economy shall be tasked with adopting, within 24 months of the entry into force of this law, the secondary legislation implementing article 26, point 1 and article 33, point 3.

Article 59

Transitional provisions

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 valid as provided for in the relevant legislation.
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.
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.

Article 60

Assessment and review

1. The responsible ministry shall draw up a report on the assessment and review of this law. Those reports shall be made public.

Article 61

Repeal upon the Date of Accession of the Republic of Albania to the European Union

1. On the date of accession of the Republic of Albania to the European Union, all provisions of this Law shall be repealed, with the exception of article 36, point 1, and article 57, point 5.
2. The Council of Ministers shall be responsible for repealing, upon the accession of the Republic of Albania to the European Union, the sub-legal acts adopted pursuant to this Law, with the exception of the sub-legal acts adopted pursuant to the articles specified in point 1 of this article.

Article 62

Entry into force and application

This law shall enter into force three (3) years after its publication in the Official Gazette.

SPEAKER OF THE PARLIAMENT

NIKO PELESHI

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I

Cybersecurity requirements relating to the properties of products with digital elements

1. Products with digital elements shall be designed, developed and produced in such a way as to ensure an appropriate level of cybersecurity based on the risks.
2. Based on the cybersecurity risk assessment referred to in point 2 of article 13 of this law and, where applicable, products with digital elements shall:

a) be made available on the market without known exploitable vulnerabilities;
b) be made available on the market with a secure default configuration, unless otherwise agreed between the manufacturer and the business user in relation to a product with digital elements manufactured to specific requirements, including the possibility to reset the product to its original state;
c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe and enabled as a default setting, with a clear and easy-to-use mechanism for disabling them, notification of available updates to users and the option to postpone them temporarily;
ç) ensure protection against unauthorised access by means of appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report any possible unauthorised access;
d) protect the confidentiality of personal or other data stored, transmitted or otherwise processed, for example by encrypting relevant data at rest or in transit using state-of-the-art mechanisms and by using other technical means;
dh) protect the integrity of personal or other data, commands, programmes and configurations that are stored, transmitted or otherwise processed against any unauthorised manipulation or modification by the user, and report any compromise;
e) process only personal or other data that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);
ë) protect the availability of essential and basic functions, including after an incident, by means of resilience measures and mitigation against denial-of-service attacks;
f) minimise the negative impact of the products themselves or connected devices on the availability of services provided by other devices or networks;
g) be designed, developed and produced to limit attack surfaces, including external interfaces;
gj) be designed, developed and produced to reduce the impact of an incident by means of appropriate mechanisms and techniques to mitigate the exploitation of vulnerabilities;
h) provide security-related information by recording and monitoring relevant internal activity, including access to or modification of data, services or functions, with a mechanism that users can disable;
(i) provide users with the ability to securely and easily permanently remove all data and settings and, where such data can be transferred to other products or systems, ensure that this is done securely.

Part II

Vulnerability-handling requirements

Manufacturers of products with digital elements shall:

1. identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used, machine-readable format covering at least the top-level dependencies of the products;
2. in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;
3. apply effective and regular tests and reviews of the security of the product with digital elements;
4. once a security update is made available, share and publicly disclose information about the vulnerabilities that have been remediated, including a description of the vulnerabilities, information enabling users to identify the affected product with digital elements, the impact and severity of the vulnerabilities, and clear, accessible information to help users remediate them. In duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making information about a remediated vulnerability public until users have had the opportunity to apply the relevant software fix or patch;
5. establish and implement a coordinated vulnerability disclosure policy;
6. take measures to facilitate the sharing of information about potential vulnerabilities in their products with digital elements and in third-party components contained in those products, including by providing a contact address for reporting vulnerabilities discovered in the product;
7. provide for secure mechanisms to distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, automatically;
8. ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a product with digital elements customised to specific requirements, free of charge and accompanied by advisory messages providing users with the relevant information, including possible action to be taken.

ANNEX II

USER INFORMATION AND INSTRUCTIONS

The product with digital elements shall be accompanied by at least the following:

1. The manufacturer”s name, registered trade name or registered trademark and postal address, email address or other digital contact details, and, where available, the website through which the manufacturer can be contacted.
2. The single point of contact through which information about vulnerabilities in the product with digital elements can be reported and obtained and where the manufacturer”s coordinated vulnerability disclosure policy can be found.
3. The name and type of the product and any additional information enabling its unique identification.
4. The intended purpose of the product with digital elements, including the security environment provided by its security attributes.

5. Any known or foreseeable circumstances relating to the use of the product with digital elements in accordance with its intended purpose or under reasonably foreseeable conditions of misuse that may lead to significant cybersecurity risks.
6. Where applicable, the internet address at which the EU declaration of conformity can be accessed.
7. The type of security technical support offered by the manufacturer and the end date of the support period during which users can expect vulnerabilities to be handled and security updates to be provided.
8. Detailed instructions or an internet address referring to such detailed instructions and information on:

a) the measures necessary during the product"s initial commissioning and throughout its lifetime to ensure its secure use;
b) how changes to the product with digital elements may affect the security of data;
c) how security-relevant updates can be installed;
ç) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;
d) how the default setting enabling the automatic installation of security updates, as required by annex I, Part I, point 2(c), to this law, can be disabled;
dh) where the product with digital elements is intended to be integrated into other products with digital elements, detailed instructions on the information necessary for the integrator to comply with the essential cybersecurity requirements set out in annex I to this law and the documentation requirements set out in annex VII to this law.

9. Information on where the software bill of materials can be accessed, if the manufacturer chooses to make it available to users.

ANNEX III

IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS

Class I

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers.
2. Stand-alone and embedded browsers.
3. Password managers.
4. Software that searches for, removes or quarantines malicious software.
5. Products with digital elements having virtual private network (VPN) functionality.
6. Network management systems.
7. Security information and event management (SIEM) systems.
8. Boot managers.
9. Public key infrastructure and software for issuing digital certificates.
10. Physical and virtual network interfaces.
11. Operating systems.
12. Routers, modems intended for connection to the internet and switches.
13. Microprocessors with security-related functionalities.
14. Microcontrollers with security-related functionalities.
15. Application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs) with security-related functionalities.
16. General-purpose virtual assistants for smart home products.

17. Smart home products with security functionalities, including smart door locks, security cameras, baby-monitoring systems and alarm systems.
18. Internet-connected toys covered by the legislation in force on toy safety that have interactive social features (for example, speaking or filming) or location-tracking features.
19. Personal wearable products intended for health monitoring (such as tracking) and not subject to the rules on medical devices or in vitro diagnostic medical devices under the legislation in force, or personal wearable products intended for use by children.

Class II

1. Hypervisors and container runtime systems supporting the virtualised execution of operating systems and similar environments.
2. Firewalls, intrusion detection and prevention systems.
3. Tamper-resistant microprocessors.
4. Tamper-resistant microcontrollers.

ANNEX IV

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

1. Hardware devices with security boxes.
2. Smart meter gateways within smart metering systems as defined in the legislation on the internal electricity market and other devices for advanced security purposes, including secure cryptoprocessing.
3. Smart cards or similar devices, including secure elements.

ANNEX V

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in article 28 of this law shall contain all of the following information:
1. The name and type of the product and any additional information enabling its unique identification.
2. The name and address of the manufacturer or its authorised representative.
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider.
4. The object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph where appropriate).
5. A statement that the object of the declaration described above complies with other legislation in force.
6. References to any relevant harmonised standards applied, or any other common specification or cybersecurity certification in relation to which conformity is declared.
7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure carried out and identification of the certificate issued.
8. Additional information:

Signed for and on behalf of:

(place and date of issue):

(name, function)

(signature):

ANNEX VI

SIMPLIFIED EU DECLARATION OF CONFORMITY

The simplified EU declaration of conformity referred to in point 20 of article 13 of this law shall be provided as follows:

Hereby, ... [manufacturer"s name] declares that the product type with digital elements ... [designation of the type of product with digital elements] complies with the rules on horizontal cybersecurity requirements for products with digital elements under this law.

The full text of the EU declaration of conformity is available at the following internet address: ...

ANNEX VII

CONTENT OF THE TECHNICAL DOCUMENTATION

The technical documentation referred to in article 31 of this law shall contain at least the following information, as applicable to the product with digital elements concerned:

1. A general description of the product with digital elements, including:
   a) its intended purpose;
   b) the software versions affecting compliance with the essential cybersecurity requirements;
   c) where the product with digital elements is a hardware product, photographs or illustrations showing its external features, marking and internal layout;
   ç) the user information and instructions referred to in annex II to this law.
2. A description of the design, development and production of the product with digital elements and of the vulnerability-handling processes, including:
   a) the information necessary about the design and development of the product with digital elements, including, where applicable, drawings and diagrams and a description of the system architecture explaining how software components are built or interact with one another and are integrated into the overall processing;
   b) the information necessary and specifications of the vulnerability-handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence that a contact address is provided for reporting vulnerabilities, and a description of the technical solutions chosen for the secure distribution of updates;
   c) the information necessary and specifications of the production and monitoring processes for the product with digital elements and validation of those processes.
3. An assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained in accordance with article 13 of this law, including how the essential cybersecurity requirements set out in part I of annex I to this law are applied.

4. The relevant information taken into account when determining the support period of the product with digital elements under point 8 of article 13 of this law.
5. A list of harmonised standards applied in full or in part, the references of which have been published in the Official Gazette, common specifications laid down in article 27 of this law, or cybersecurity certification schemes in accordance with point 8 of article 27 of this law and, where those harmonised standards, common specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential cybersecurity requirements set out in parts I and II of annex I to this law, including a list of other relevant technical specifications applied. In the case of harmonised standards, common specifications or cybersecurity certification schemes applied in part, the technical documentation shall specify the parts that have been applied.
6. Test reports carried out to verify the conformity of the product with digital elements and its vulnerability-handling processes with the applicable essential cybersecurity requirements set out in parts I and II of annex I to this law.
7. A copy of the EU declaration of conformity.
8. Where applicable, the software bill of materials, upon a reasoned request from a market surveillance responsible structure , where necessary to enable that authority to check compliance with the essential cybersecurity requirements set out in annex I to this law.

ANNEX VIII

CONFORMITY ASSESSMENT PROCEDURES

Part I
Conformity assessment procedure based on internal control (based on Module A)

1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4 of this Part and ensures and declares, under its sole responsibility, that the products with digital elements meet all the essential cybersecurity requirements set out in part I of annex I to this law and that the manufacturer meets the essential cybersecurity requirements set out in part II of annex I to this law.
2. The manufacturer shall draw up the technical documentation described in annex VII to this law.
3. Design, development, production and vulnerability handling of products with digital elements.
The manufacturer shall take all necessary measures so that the design, development, production and vulnerability-handling processes, and their monitoring, ensure that products with digital elements manufactured or developed and the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in parts I and II of annex I to this law.
4. CE marking and EU declaration of conformity.
4.1. The manufacturer shall affix the CE marking to each individual product with digital elements that meets the applicable requirements laid down in this law.
4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with article 28 of this law and keep it, together with the technical documentation, available to the national authorities for 10 years after the product has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.
5. Authorised representatives.

The manufacturer"s obligations laid down in point 4 of this Part may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the written mandate.

Part II

EU-type examination (based on Module B)

1. EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product with digital elements and the vulnerability-handling processes put in place by the manufacturer, and certifies that the product with digital elements meets the essential cybersecurity requirements set out in part I of annex I to this law and that the manufacturer meets the essential cybersecurity requirements set out in part II of annex I to this law.
2. EU-type examination shall be carried out by assessing the adequacy of the technical design and development of the product with digital elements through examination of the technical documentation and supporting evidence referred to in point 3 of this Part, and examination of samples of one or more critical parts of the product (combination of production type and design type).
3. The manufacturer shall lodge an application for EU-type examination with a single notified body of its choice.
The application shall include:
3.1. the name and address of the manufacturer and, if the application is lodged by an authorised representative, the name and address of the authorised representative;
3.2. a written declaration that the same application has not been lodged with any other notified body;
3.3. the technical documentation, which shall make it possible to assess the conformity of the product with digital elements with the applicable essential cybersecurity requirements set out in Part I of annex I to this law and the manufacturer's vulnerability-handling processes set out in part II of annex I to this law, and shall include an adequate analysis and assessment of the risks. The technical documentation shall specify the applicable requirements and cover, insofar as relevant to the assessment, the design, production and operation of the product with digital elements. Where applicable, the technical documentation shall contain at least the elements set out in annex VII to this law;
3.4. supporting evidence for the adequacy of the technical solutions adopted for the design and development and of the vulnerability-handling processes. That supporting evidence shall mention any documents used, in particular where the relevant harmonised standards or common specifications have not been applied in full. Where necessary, the supporting evidence shall include the results of tests carried out by the manufacturer's appropriate laboratory or by another testing laboratory on its behalf and under its responsibility.
4. The notified body shall:
4.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with digital elements in relation to the essential cybersecurity requirements set out in part I of annex I to this law and of the vulnerability-handling processes put in place by the manufacturer in relation to the essential cybersecurity requirements set out in part II of annex I to this law;
4.2. verify that the samples have been developed or manufactured in conformity with the technical documentation and identify the elements designed and developed in accordance with the applicable provisions of the relevant harmonised standards or technical specifications, as well as the elements designed and developed without applying the relevant provisions of those standards;

4.3. carry out, or have carried out, the appropriate examinations and tests to check that, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards or technical specifications for the requirements set out in annex I to this law, those solutions have been applied correctly;
4.4. carry out, or have carried out, the appropriate examinations and tests to check that, where the solutions in the relevant harmonised standards or technical specifications for the requirements set out in annex I to this law have not been applied, the solutions adopted by the manufacturer meet the relevant essential cybersecurity requirements;
4.5. agree with the manufacturer on the location where the examinations and tests will be carried out.
5. The notified body shall draw up an assessment report recording the activities undertaken in accordance with point 4 of this Part and their results. Without prejudice to its obligations towards the notifying authorities, the notified body shall publish the contents of that report, in whole or in part, only with the manufacturer's agreement.
6. Where the type and the vulnerability-handling processes meet the essential cybersecurity requirements set out in annex I to this law, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, any conditions for its validity and the data necessary to identify the approved type and the vulnerability-handling processes. The certificate may have one or more annexes attached to it.
The certificate and its annexes shall contain all relevant information to allow the conformity of products with digital elements manufactured or developed in conformity with the examined type and vulnerability-handling processes to be assessed and to allow in-service control.

Where the type and the vulnerability-handling processes do not meet the applicable essential cybersecurity requirements set out in annex I to this law, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.
7. The notified body shall keep itself apprised of any changes in the state of the art indicating that the approved type and vulnerability-handling processes may no longer comply with the applicable essential cybersecurity requirements set out in annex I to this law, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.
The manufacturer shall inform the notified body holding the technical documentation relating to the EU-type examination certificate of all changes to the approved type and vulnerability-handling processes that may affect compliance with the essential cybersecurity requirements set out in annex I to this law or the conditions for the certificate's validity. Such changes shall require additional approval in the form of an addition to the original EU-type examination certificate.
8. The notified body shall carry out periodic audits to ensure that the vulnerability-handling processes referred to in part II of annex I to this law are implemented appropriately.
9. Each notified body shall inform its notifying authorities of EU-type examination certificates and any additions thereto that it has issued or withdrawn and shall make available to those authorities, periodically or upon request, a list of certificates and additions that it has refused, suspended or otherwise restricted.
Each notified body shall inform the other notified bodies of EU-type examination certificates and any additions thereto that it has refused, withdrawn, suspended or otherwise restricted and, upon request, of certificates and additions that it has issued.
The responsible ministry and notified bodies may obtain a copy of EU-type examination certificates and any additions thereto. Upon request, the responsible ministry may obtain a copy of the technical

documentation and the results of examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file, including the documentation submitted by the manufacturer, until the certificate expires.

10. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions, together with the technical documentation, available to the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.

11. The manufacturer"s authorised representative may lodge the application referred to in point 3 of this Part and fulfil the obligations laid down in points 7 and 10 of this Part, provided that the relevant obligations are specified in the written mandate.

Part III

Conformity to type based on internal production control (based Module C)

1. Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 3 of this Part and ensures and declares that the products with digital elements conform to the type described in the EU-type examination certificate and meet the essential cybersecurity requirements set out in Part I of annex I to this law, and that the manufacturer meets the essential cybersecurity requirements set out in part II of annex I to this law.

2. Production.

The manufacturer shall take all necessary measures so that the production process and its monitoring ensure that the products with digital elements manufactured conform to the approved type described in the EU-type examination certificate and to the essential cybersecurity requirements set out in Part I of annex I to this law, and that the manufacturer meets the essential cybersecurity requirements set out in part II of annex I to this law.

3. CE marking and EU declaration of conformity.

3.1. The manufacturer shall affix the CE marking to each individual product with digital elements that conforms to the type described in the EU-type examination certificate and meets the applicable requirements laid down in this law.

3.2. The manufacturer shall draw up a written EU declaration of conformity for a product model and keep it available to the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product model for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

4. Authorised representative.

The manufacturer"s obligations laid down in point 3 of this Part may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the written mandate.

Part IV

Conformity based on full quality assurance (based on Module H)

1. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5 of this Part and ensures and declares, under its sole responsibility, that the products with digital elements or product categories meet the

essential cybersecurity requirements set out in part I of annex I to this law and that the vulnerability-handling processes put in place by the manufacturer meet the requirements set out in part II of annex I to this law.

2. Design, development, production and vulnerability handling of products with digital elements.

The manufacturer shall operate an approved quality system, as specified in point 3 of this Part, for the design, development, inspection and final testing of products with digital elements and for vulnerability handling, shall maintain its effectiveness throughout the support period and shall be subject to surveillance as specified in point 4 of this Part.

3. Quality system.

3.1. The manufacturer shall lodge an application for assessment of its quality system with the notified body of its choice for the products with digital elements concerned.

The application shall include:

a) the name and address of the manufacturer and, if the application is lodged by an authorised representative, the name and address of the authorised representative;

b) the technical documentation for a model of each category of products with digital elements intended to be manufactured or developed. Where applicable, the technical documentation shall contain at least the elements set out in annex VII to this law;

c) the documentation relating to the quality system; and

ç) a written declaration that the same application has not been lodged with any other notified body.

3.2. The quality system shall ensure that the products with digital elements comply with the essential cybersecurity requirements set out in part I of annex I to this law and that the vulnerability-handling processes put in place by the manufacturer comply with the requirements set out in part II of annex I to this law.

All elements, requirements and provisions adopted by the manufacturer shall be documented systematically and in an orderly manner in the form of written policies, procedures and instructions. The quality system documentation shall allow a consistent interpretation of quality programmes, plans, manuals and records.

In particular, it shall contain an adequate description of:

a) the quality objectives and organisational structure, responsibilities and powers of senior management with regard to product design, development, product quality and vulnerability handling;

b) the technical design and development specifications, including the standards to be applied and, where the relevant harmonised standards or technical specifications are not applied in full, the means to be used to ensure that the applicable essential cybersecurity requirements set out in part I of annex I to this law are met for products with digital elements;

c) the procedural specifications, including the standards to be applied and, where the relevant harmonised standards or technical specifications are not applied in full, the means to be used to ensure that the essential cybersecurity requirements set out in part II of annex I to this law that apply to the manufacturer are met;

ç) the design and development control, design and development verification techniques, processes and systematic actions to be used during the design and development of products with digital elements belonging to the product category covered;

d) the corresponding manufacturing, quality control and quality assurance techniques, processes and systematic actions to be used;

dh) the examinations and tests to be carried out before, during and after production, and the frequency with which they are to be carried out;

e) quality records, such as inspection reports and test data, calibration data and personnel qualification reports;

f) the means of monitoring achievement of the required design and product quality and the effective operation of the quality system.

3.3. The notified body shall assess the quality system to determine whether it meets the requirements referred to in point 3.2.

It shall presume conformity with those requirements in respect of elements of the quality system that comply with the corresponding specifications of the national standard implementing the relevant harmonised standard or technical specification.

In addition to experience in quality management systems, the audit team shall have at least one member with experience as an assessor in the relevant product field and product technology and knowledge of the applicable requirements laid down in this law. The audit shall include an assessment visit to the manufacturer"s premises, where such premises exist. The audit team shall review the technical documentation referred to in point 3.1(b) to verify the manufacturer"s ability to identify the applicable requirements laid down in this law and to carry out the necessary examinations to ensure that the product with digital elements complies with those requirements.

The manufacturer or its authorised representative shall be notified of the decision.

The notification shall contain the audit conclusions and the reasoned assessment decision.

3.3. The manufacturer shall undertake to fulfil the obligations arising from the quality system as approved and to maintain it so that it remains adequate and efficient.

3.4. The manufacturer shall keep the notified body that approved the quality system informed of any intended changes to that system.

The notified body shall assess any proposed change and decide whether the modified quality system will continue to meet the requirements referred to in point 3.2 or whether a reassessment is necessary. It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.

4. Surveillance under the responsibility of the notified body.

4.1. The purpose of surveillance is to ensure that the manufacturer duly fulfils the obligations arising from the approved quality system.

4.2. For assessment purposes, the manufacturer shall allow the notified body access to the design, development, production, inspection, testing and storage sites and shall provide it with all necessary information, in particular:

a) the quality system documentation;
b) the quality records provided for by the design part of the quality system, such as the results of analyses, calculations and tests;
c) the quality records provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data and relevant personnel qualification reports.

4.3. The notified body shall carry out periodic audits to ensure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.

5. CE marking and EU declaration of conformity.

5.1. The manufacturer shall affix the CE marking and, under the responsibility of the notified body referred to in point 3.1, that body's identification number to each individual product with digital elements that meets the requirements set out in part I of annex I to this law.

5.2. The manufacturer shall draw up a written EU declaration of conformity for each product model and keep it available to the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product model for which it has been drawn up.

A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

6. For a period ending at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, the manufacturer shall keep the following available to the national authorities:

a) the technical documentation referred to in point 3.1;
b) the documentation relating to the quality system referred to in point 3.1;
c) the approved change referred to in point 3.5;
ç) the decisions and reports of the notified body referred to in points 3.5 and 4.3.

7. Each notified body shall inform the notifying authority of quality system approvals issued or withdrawn and shall make available to the notifying authorities, periodically or upon request, a list of quality system approvals refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies of quality system approvals it has refused, suspended or withdrawn and, upon request, of quality system approvals it has issued.

8. Authorised representative.

The manufacturer"s obligations laid down in points 3.1, 3.5, 5 and 6 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the written mandate.