REPUBLIC OF ALBANIA

PARLIAMENT

LAW

NO. 25/2024

FOR CYBER SECURITY [1]

In support of articles 78, article 81, point 1 and 83, point 1, of the Constitution, with the proposal of the Council of Ministers,

PARLIAMENT

OF REPUBLIC OF ALBANIA

DECREED:

CHAPTER I
GENERAL PROVISIONS

Article 1
Object of the law

1. The object of this law is to determine the rights and obligations of public and private entities, which administer information infrastructures, communication networks and their systems, the violation or destruction of which would have an impact on the health, safety, economic well-being of citizens and the effective functioning of the economy in the Republic of Albania.

This law is partially aligned with Directive (EU) no. 2022/2555 of the European Parliament and Council, dated December 14, 2022 "On measures for a high common level of cyber security throughout the European Union, amending Regulation (EU) no. 910/2014 and Directive (EU) no. 2018/1972, and repealing Directive (EU) no. 2016/1148 with effect from October 18, 2024, (NIS 2)", Official Journal of the European Union, Series L, no. 333, dated 27.12.2022, page 80-152.

2. This law also defines:
   a. the authority responsible for Cyber Security in the Republic of Albania, which is also the single point of contact for cyber security issues as well as other responsible security and defense institutions that interact on cyber security issues in the country.
   b. cyber security incident response teams such as National CSIRT, CERT, sectoral CSIRT-s.
   c. the authority responsible for drafting the National Cyber Security Strategy;
   d. security measures and cybersecurity risk management measures by the entities mentioned in Annex I and Annex II of this law.
   e. reporting of cyber security incidents by the entities mentioned in Annex I and Annex II of this law.
   f. rules and obligations for sharing cyber security information;

Article 2
Purpose of the law

The purpose of this law is to define measures in order to achieve a high level of cyber security for networks and information systems in the Republic of Albania.

Article 3
Scope

The provisions of this law apply to all those public and private entities that administer information systems and networks according to the definitions made in Annex 1 and Annex 2 of this law.

Article 4
General principles of cyber security

1. The processing of personal data is carried out in accordance with the provisions defined in the legislation for the protection of personal data.
2. In accordance with the provisions set forth in this law, the principle of technology neutrality shall be applied to the fullest extent possible, whereby the entities governed by this law are free to select the most appropriate technology for their needs without imposing or discriminating against any particular type of technology, thereby encouraging the adoption of European and international standards and essential technical specifications for the security of network and information systems.

Article 5
Definitions

In terms of this law, the following terms have the following meanings:

1. "**Authority responsible for Cyber Security",** is the National Authority for Cyber Security, the public body responsible for the implementation and supervision of this law, hereinafter the Authority.
2. "**Accreditation"** according to this law has the same meaning as the definition given in the legislation in force for the accreditation of conformity assessment bodies in the Republic of Albania.
3. **"CERT",** is the Cyber Security Emergency Response Team at the Authority.
4. **"National CSIRT",** is the Cyber Security Incident Response Team, under the Authority.
5. "**Sectoral CSIRT",** is the individual or team responsible for responding to cybersecurity incidents within the respective sector, as defined in the annexes of this law, established within an operator managing critical and important information infrastructure or the responsible institution in charge.
6. "**Government CSIRT**", is the sectoral CSIRT which manages all critical and important information infrastructures for the government sector.
7. "**CSIRT near the operators**", is the response team to Cyber Security Incidents, near the operators of critical and important information infrastructures.
8. "**Cybersecurity certificate",** is a document issued by a cybersecurity conformity assessment body, verifying that an ICT product, service, or process has been assessed for compliance with specific security requirements outlined in the cybersecurity certification scheme.
9. "**ENISA"**, is the Cyber Security Agency of the European Union.
10. "**Cybersecurity emergency",** is the situation during which the security of information in information systems, or the security of electronic communications networks is compromised, putting the public interest of the Republic of Albania at risk.
11. "**Cooperation Group"** is a body created by Directive (EU) no. 2022/2555 of the European Parliament and Council, dated 14 2022, with the aim of facilitating the strategic agreement and the exchange of information between the parliament of December of members of EU
12. "**Cyber space",** is the digital environment capable of creating, processing and exchanging electronic communication of information created by networks and information systems even without being connected to the Internet.
13. "**Cyber security incident",** is any event that compromises the availability, authenticity, integrity, confidentiality of data stored, transmitted, or processed or services provided, or accessible through networks and information systems.
14. "**Critical information infrastructure**", is the totality of networks and information systems, owned by a public or private authority, that provide services, the violation or destruction of which would have a serious impact on the health, safety, economic well-being of citizens and the effective functioning of the economy in the Republic of Albania.

15. "**Important information infrastructure",** is the totality of networks and information systems owned by a public or private authority, which is not part of the critical information infrastructure, but which may endanger or limit the provision of the service and the continuity of work , in case of breach of information security.
16. "**Cyber threat",** is a possible event or action that can damage, interrupt, or negatively affect networks and information systems, for their users and other persons.
17. "**Cyber crisis",** is the situation during which the security of information in information systems or the security of electronic communications networks is seriously endangered, putting the public interest of the Republic of Albania at risk.
18. **"Log",** message or information about events related to cyber security.
19. "**Cybersecurity measures**" mean the set of actions for increasing information security in information systems and the availability and reliability of communication network services in cyberspace.
20. **"Online search engine"** refers to a digital service that allows users to input queries to perform searches, in principle, on all web pages, or on all web pages in a specific language, based on a query for any topic in the form of a keyword, voice command, phrase, or other input, and in any format in which information is related to the desired content."
21. "**Operator of the critical information infrastructure",** is any natural or legal person who administers the critical information infrastructure and meets the requirements defined in this law.
22. "**Operator of the important information infrastructure",** is any natural or legal person, who administers the important information infrastructure and meets the requirements defined in this law.
23. "**Conformity Assessment Body**", is a natural or legal person, national or international, accredited by the institution responsible for accreditation, to carry out conformity assessments and testing of ICT products, services and processes, as well as the assessment of cyber security measures implemented by critical and important information infrastructures.
24. "**DNS service provider",** means an entity that provides:
a) publicly available recursive domain name resolution services for internet end-users; or
b) authoritative domain name resolution services for third-party use, except for root name servers.
25. "**Managed Service Provider**" refers to an entity that provides services related to the installation, management, operation, or maintenance of IT products, networks, infrastructure, applications, or any other information networks and systems, through active assistance or administration performed either on the premises of the clients or remotely.
26. "**Managed Security Service Provider**" means a managed service provider that performs or provides assistance with activities related to the management of cybersecurity risk;
27. "**Research Organization"** means an entity primarily engaged in applied or experimental research development with the intent to exploit the results of that research for commercial purposes, excluding educational institutions.

28. “**Internet exchange point”,** means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

29. **"Playbooks”** constitute a guide that outlines a well-defined procedure to be followed for the management of each category of cybersecurity incident

30. "**ICT Product",** means an element or a group of elements of a network or information system.

31. **“ICT process",** means a set of activities to design, develop, provide, or maintain an ICT product or service.

32. “**Illegal content for children** " according to this law has the same meaning as the definition given in the legislation in force on the rights and protection of the child.

33. **“Social Networking Service Platform"** means a platform that enables end-users to connect, share, discover, and communicate with each other through various devices, especially through chats, posts, videos, and recommendations.

34. “**Top high-Level Domain Name Registry .al**" or "**TLD.al Domain Name Registry"** refers to the registry containing the internet domain names registered in the Republic of Albania with the .al top-level domain, administered by the Authority responsible for electronic and postal communications, which drafts, approves, and enforces specific regulations for this purpose. The registry includes the names of ccTLD.al domains (and subdomains), their registrants' data, the history of actions with .al domains, and the technical system of ccTLD.al, which encompasses the operation of servers and other necessary equipment, maintenance of databases, and distribution of TLD zone files to enable access to .al domain names on the internet, and so on, all of which are included in the aforementioned regulation.

35. **"Network and information system"** is:

a) electronic communications network according to the provisions made in the law on electronic communications in force;

b) any device or group of connected or interconnected devices, one or some of them, perform the automatic processing of digital data, through a program.

c) digital data stored, processed, received or transmitted by elements provided for in points (a) and (b) for their operation, use, protection and maintenance.

36. "**Cyber security risk",** is an identifiable event with a possible negative effect on the security of networks and information systems.

37. “**Network of CSIRTs"** is the network created by Directive (EU) no. 2022/2555 of the European Parliament and Council, dated December 14, 2022, consisting of the national CSIRTs of the EU member states with the aim of promoting of fast and effective operational cooperation between them.

38. "**European Network of Cyber Crisis Liaison Organizations (EU-CyCLONe)"**, is the network created by Directive (EU) no. 2022/2555 of the European Parliament and Council, dated December 14, 2022 with the aim of supporting the coordination of management of large-scale cyber security incidents and crises at the operational level and to ensure the exchange of information between EU Member States, EU institutions, bodies, offices and agencies.
39. **"Content Distribution Network"** means a geographically distributed network of servers designed to ensure the availability, accessibility, or rapid distribution of digital content and services to internet users on behalf of content providers and service providers.
40. "**Public Electronic Communications Network"** has the same meaning as defined in the current legislation for electronic communications.
41. "**Cyber resilience",** refers to the ability of information systems to protect data from cyberattacks, as well as the capability to restore normal operations within a time frame that does not adversely affect the activities of a critical infrastructure operator or significant information entity, in the event of a cyberattack."
42. "**Security of the network and information systems",** is the ability of the network and information systems to resist at a certain level of security any action that compromises the availability, authenticity, integrity and confidentiality of data stored, transmitted or processed and the corresponding services provided through this network or information systems.
43. **"Cyber security"** is the set of actions necessary to protect networks and information systems, users of these networks and systems, as well as other persons affected by cyber threats.
44. "**National Strategy for Cyber Security",** is a policy document that defines objectives, plans and strategic priorities for the security of networks and information systems and the creation of safe cyber spaces for society, at the national level.
45. **"Cybersecurity certification scheme",** is the complete set of rules, technical requirements, standards, and procedures applied for certifying or assessing the conformity of products, services, and processes related to cybersecurity in ICT.
46. **"Standard"**, according to this law, has the same meaning as the definition given in the legislation in force for standardization.
47. **"Technical specification",** is a document which defines the required characteristics of a product such as levels of quality, performance, and safety, including the requirements applicable to the product in relation to the name under which the product is sold, terminology, symbols, test methods, packaging, marking, or labelling and conformity assessment procedures. This term also covers production methods and processes.
48. **"The Domain Name System (DNS)",** is a system that distributes names hierarchically and facilitates the identification of internet services and resources, thereby enabling end-user devices to utilize internet routing and connection services to access those services and resources."

49. "**Other responsible subjects in the field of cyber security",** are the superior or regulatory institutions responsible for the field of activity of the sectors, according to which critical and important information infrastructures are categorized.
50. **"Proactive scanning"** implies the execution of one or more advanced preparatory actions that enable the identification, detection, and memorization of risks with significant impact before their occurrence.
51. **"Digital service",** means any information society service as defined in the law on electronic commerce.
52. **"ICT service",** means a service that consists entirely or mainly in the transmission, storage, reception, or processing of information by means of network and information systems.
53. **"Cloud Computing Services"** means a digital service that enables on-demand administration and remote access to a scalable and elastic group of individual computer resources, including the location where such resources are distributed across multiple locations.
54. **"Data Centre Service"** means a service that includes structures or groups of structures dedicated to centralizing the accommodation, interconnection, and operation of information technology and network equipment providing data storage, data processing, and transport services, along with all facilities and infrastructures for energy distribution and environmental control.
55. "**Electronic Communications Service"** has the same meaning as defined in the current legislation for electronic communications.
56. "**Online market"**, It is a service that utilizes software, including a website, parts of a website, or an application, operated by or on behalf of a merchant that allows consumers to remotely conclude contracts with merchants or other consumers."
57. "**Cybersecurity incident handling**", are all procedures necessary for the prevention, identification, analysis, response, and recovery of a cyber security incident.
58. "**Vulnerability",** is a weakness, sensitivity or defect in ICT products or services that can be exploited by a cyber threat.

CHAPTER II

INSTITUTIONAL ORGANIZATION AND RESPONSIBLE ENTITIES FOR CYBER SECURITY

Article 6
National Cyber Security Strategy

1. The Authority is the institution responsible for drafting and monitoring the National Cyber

Security Strategy, which coordinates work with other institutions responsible for cyber security.
2. In the drafting of the National Cyber Security Strategy, the following are defined:
a) the objectives and priorities of the cyber security strategy, including the sectors mentioned in Annex I and Annex II of this law;
b) a legal framework to achieve the objectives and priorities mentioned in letter "a", point 2 of this article as well as the policies mentioned in point 3 of this article.
c) the legal framework, which defines the roles and responsibilities of the relevant actors at the national level, supporting collaboration and coordination nationally among competent authorities, the single point of contact, and Computer Security Incident Response Teams (CSIRTs) pursuant to this law, as well as the coordination of and cooperation in international matters;
d) training, awareness-raising, and education programs;
e) measures ensuring readiness, response, and recovery from incidents, including cooperation between the public and private sectors;
f) a plan for the identification of cybersecurity-related assets and the assessment of cybersecurity risks;
g) a list of various actors to be involved in the implementation of the strategy.
3. Specifically, the strategy includes the following policies:
a) addressing cybersecurity in the supply chain for Information and Communication Technology (ICT) products and ICT services used by entities to provide their services;
b) vulnerability management, including promotion and coordination for vulnerability discovery;
c) promoting the development and integration of advanced technologies aimed at implementing modern cybersecurity risk management measures;
d) promoting and developing cybersecurity training, education, skills, awareness, research and development initiatives, as well as guidelines for best practices and controls in cyber hygiene, for citizens, stakeholders, and entities governed by this law;
e) supporting academic and research institutions to develop, improve, and promote cybersecurity tools and network infrastructure;
f) promoting active cyber defense.
4. The National Cybersecurity Strategy is developed for a five-year period and approved by a decision of the Council of Ministers.
5. The strategy is accompanied by an action plan, which is developed by the Authority in coordination with the responsible cybersecurity institutions, for a period of at least two years and approved by a decision of the Council of Ministers.

Article 7
Responsible Authority for Cyber Security

1. The Authority is the regulatory body responsible for the supervision and implementation of cyber security legislation in the Republic of Albania.

2. The Authority is a public legal entity, headquartered in Tirana, subordinate to the Prime Minister, which is financed from the state budget and other legal sources.
3. The Authority in relations with third parties is represented by the General Director.
4. The working relations of the General Director, the employees of the Authority are regulated based on the provisions of law no. 7961, dated 12.7.1995 "Labor Code of the Republic of Albania", as amended.
5. The General Director and the employees of the technical units of the content of the Authority, in addition to the salary according to the salary categories determined by the decision of the Council of Ministers, benefit from an allowance for a special nature of work, in the amount of up to 800,000 (eight hundred thousand) ALL per month. The measure of the allowance for special nature of work for each category is determined by the decision of the Council of Ministers.
6. Part of the structure and organization of the National Cyber Security Authority is the National Cyber Security Operational Center responsible for monitoring cyber security, simulations and taking additional corrective measures for a faster and more efficient response to cyber incidents or attacks.
7. The organization and operation of the Authority is approved by decision of the Council of Ministers.

Article 8
Appointment, release or dismissal of the General Director

1. The General Director of the Authority is appointed, released and dismissed by the Prime Minister.
2. The General Director of the Authority must meet the following criteria:
a) to be an Albanian citizen;
b) to have full ability to act:
c) to have a seventh level diploma of the Albanian Framework of Qualifications, "Scientific Master" or "Professional Master's degree obtained at the end of the second cycle studies with 120 credits and with a normal duration of 2 academic years" or a valid equivalent, according to the legislation on higher education, in the field of information and communication technologies (ICT) or electronic engineering.
d) to have at least 10 years experience in profession;
e) to stand out for professional skills in the field of cyber security and to be international certified in the cyber security field;
f) the disciplinary measure of dismissal was not taken against him, which has not been extinguished according to the legislation in force;
g) not having been convicted by a final court decision for committing a criminal offense;

h) there should be no conflict of interest in the exercise of duty according to the provisions made in the legislation in force for the prevention of conflict of interest in the exercise of public functions.

3. The General Director of the Authority is relieved of duty when:

a) the conditions for the full old-age pension are met;

b) declared unfit for work by the competent medical commission;

c) is in a situation of continuous conflict of interest;

d) resign from office.

4. The General Director of the Authority is dismissed from office when:

a) is punished by a final court decision for the commission of a crime or for the commission of an intentional criminal misdemeanor;

b) strategic objectives are not met due to its low performance;

c) commits serious violations in duty.

5. Serious violations in duty are considered:

a) repeated violation of ethical rules according to the legislation in force;

b) violation of rules for the preservation of classified information;

c) exercise of duty under conditions of conflict of interest.

Article 9
Competences of the National Cyber Security Authority

The National Authority for Cyber Security, in accordance with the provisions made in this law, exercises the following competences:

a) identifies and classifies critical and important information infrastructures.

b) acts as a central point of contact at the national and international level, as well as coordinates the work with other institutions in the field of cyber security for the resolution of cyber incidents.

c) acts in the capacity of the National CSIRT and CERT;

d) determines and controls the implementation of cyber security measures, that shall be applied by the operators of critical and important information infrastructures;

e) cooperates and exchanges important information with the operators of critical and important information infrastructures, regarding the data in the systems, when they are endangered due to a cyber incident.

f) It assists critical and significant information infrastructure operators in managing cyber incidents.

g) performs active monitoring of critical and significant information infrastructure through information obtained from external platforms established by the Authority, as well as from internal platforms upon request from information infrastructure operators, aiming to detect and prevent malicious activities;

h) it assesses and analyzes the level of cybersecurity of critical and important information infrastructure systems through continuous checks and simulations. Additionally, it determines supplementary measures for information infrastructure operators to ensure a swift and effective response to cyber incidents or attacks. The methodology for assessing and analyzing cyber security is approved by the decision of the Council of Ministers.

i) registers cybersecurity conformity assessment bodies for the evaluation of cybersecurity measures;

j) establishes and manages the register of documentation of cybersecurity incidents;

k) periodically reports on cyber incidents to ENISA and other international bodies as part of the commitments of the Republic of Albania regarding cybersecurity matters;

l) conducts awareness and education activities in the field of cybersecurity for all societal groups;

m) the Authority, through the Director General's Order and in collaboration with operators of critical and important information infrastructures, conducts and promotes, as deemed necessary, training for the personnel of these operators to ensure highly effective fulfillment of their duties;

n) undertakes necessary measures, collaborates, and coordinates efforts with institutions responsible for the security and protection of children and young people to establish a secure online cyber environment within the Republic of Albania.

Article 10
Reporting on the State of Cybersecurity

1. With the aim of assessing the level of cybersecurity in the country, the Authority prepares an annual report which includes an assessment of:

a) the cybersecurity risk in the country;

b) the cybersecurity capabilities in the country;

c) the technical, financial, and human resources available to information infrastructure, cybersecurity policies, and the implementation of monitoring measures;

d) an assessment of the overall level of cybersecurity awareness and cyber hygiene among citizens and legal entities;

e) the level of growth in cybersecurity capacity.

2. The report also includes specific policy recommendations for enhancing the level of cybersecurity in the country and a summary of findings for the one year period.

3. Within the date of March 31 of the following year, the report prepared in accordance with points 1 and 2 of this article shall be presented to the Prime Minister of the Republic of Albania.

Article 11
Other entities responsible for cyber security

Other entities responsible for the security of networks and information systems in the Republic of Albania are as follows:

a) Institutions responsible for cyber security and protection:
i. Ministry responsible for the energy and transport, telecommunications, and postal service;
ii. Ministry responsible for public order and security;
iii. Ministry responsible for finance;
iv. Ministry responsible for economy;
v. Ministry responsible for the health care;
vi. Ministry responsible for the environment, tourism, territory protection and other related functions;
vii. Ministry responsible for agriculture and other related functions.
viii. National Agency for Information Society (NAIS);
ix. The state police, the institution responsible for maintaining order and public safety.
x. Electronic and Postal Communications Authority (EPCA)
xi. Other institutions responsible for the storage and processing of government data.
xii. Any other independent public institution that administers information infrastructures in the sense of this law.
b) Entities responsible for providing the services of the sectors, such as :
i. Entities that provide services in the energy sectors, including the electricity, oil gas and nuclear energy sectors;
ii. Entities that provide services in the air, sea, railway, road, postal and telecommunication transport sectors;
iii. Entities that provide services in the sectors of economy, finance, financial market infrastructure, the banking sector, as well as microfinance sectors;
iv. Entities providing services in the insurance market, insurance companies;
v. Entities providing services in the health care and assistance sectors authorized and accredited by the responsible authorities;
vi. Entities that provide services in the environmental, tourism and territorial protection sectors, and territorial authorities responsible for the supply and distribution of drinking water;
vii. Entities that provide services in the sectors of digital infrastructure, telecommunications, and digital services;
viii. Entities that provide services in the academic sector, when performing critical research activities;
ix. As well as any other sector that provides services through networks and information systems subject to this law.

Article 12
Identification of operators of critical and important information infrastructures

1. The Authority performs the identification of critical and important information infrastructures continuously in cooperation and coordination with other entities responsible for cyber security;
2. The identification of operators of critical and important information infrastructures is carried

out on the basis of a methodology, which is approved by decision of the Council of Ministers, according to the determinations made in Annex I and Annex II of this law;
3. The criteria on which the identification of critical and important information infrastructures is based are as follows:
a) the service provided is critical or important for the maintenance of critical social and economic activities;
b) the provision of that service depends on electronic communication networks and information systems;
c) an incident has significant disruptive effects on the provision of that service.
4. The entities identified as critical or important information infrastructure have the obligation to accurately report the following information to the Authority:
a) name of the entity;
b) address;
c) when applicable, the sector and sub-sector according to the determinations made in Annexes I and II of this law;
d) when applicable, a list of the states where they provide services that are part of the scope of this law.
5. The list of critical and important information infrastructures is confidential and updated at least once every two years under the direction of the Authority and approved by decision of the Council of Ministers.

Article 13
Competences and responsibilities of the National CSIRT

The Cyber Security Incident Response Team, near the Authority fulfills the following competences and responsibilities:
a) actively communicates through an appropriate, secure and stable communication and information infrastructure, through which the exchange of information is carried out with the operators of critical and important information infrastructures, in order to ensure the continuity of their activity at all times and without interruption;
b) interacts with the operators of critical and important information infrastructures, through platforms dedicated to the distribution of information and the reporting of cyber incidents for their management and handling.
c) monitors, analyzes, and manages cyber threats, vulnerabilities, and incidents at the national level, and provides technical assistance to critical and significant information infrastructures upon request from information infrastructure operators."
d) acts in the capacity of coordinator for the identification of vulnerabilities in networks and information systems.
e) monitors in cooperation with the operators of critical and important information infrastructures, networks and systems in their infrastructures on cyber security incidents or cyber-attacks;

f) handles cyber incidents in cooperation with the operators of critical and important information infrastructures and provides concrete solutions based on the policies and measures defined in this law, as well as cooperates with the relevant law enforcement institutions when suspects for elements of cybercrime;
g) Warns, notifies, and distributes information to critical and important information infrastructures as well as responsible entities, regarding potential risks, vulnerabilities and cyber incidents.
h) Collects and analyzes data through digital investigation and provides dynamic risk and incident analysis, as well as carries out awareness of the current cyber security situation.
i) ensures the storage of logs of recorded or reported incidents for a period specified in the regulation approved by order of the General Director of the Authority.
j) permforms proactive scans of networks and information systems to identify vulnerabilities, with high possible impact by informing in advance the information infrastructure operator about all the technical and legal elements of performing these scans.
k) It assesses when the infrastructure is in a high-risk situation and performs reactive actions, in cooperation with the infrastructure after notifying the occurrence of the incident when the service provided by the infrastructure has stopped functioning for more than 4 hours. The methodology for assessing the risk of infrastructure is determined by the guidance of the Director-General of the Authority after consulting with operators of critical and important information infrastructures.
l) Controls the implementation of cyber security measures by operators of critical and important information infrastructures.
m) Responds to any infrastructure, implementing security procedures, to actively support incident resolution.
n) Analyzes and prepares measures of a special nature according to the cyber incident and communicates them to the sectoral CSIRTs and CSIRTs near the operators of critical and important information infrastructures.
o) It prepares and approves, through an order from the Director General of the Authority, guidelines, policies, and regulations to harmonize and enhance the procedures for managing cyber incidents.
p) Keeps the electronic register of contact points with the data defined in letter "i", of Article 16 and in article 18 of this law.
q) Simulates networks and systems to find infrastructure vulnerabilities by notifying operators in advance.
r) Analyzes the incident to find its cause as well as coordinates the activity with the operators, sectorial CSIRTs, international and governmental institutions when it deems it reasonable;
s) The National CSIRT is part of the network of international CSIRTs and offers joint assistance based on its capacities and competences to the members of this network upon request.
t) Coordinates with the State Police and any responsible institution to preserve and facilitate the collection of evidence when there is suspicion of cybercrime elements or other related criminal acts within information infrastructures.

Article 14
Vulnerability discovery

1. The national CSIRT identifies, analyzes, and provides assistance to information infrastructure operators in the case of a primarily identified or reported vulnerability by information infrastructure operators.
2. The national CSIRT, in its role as the coordinator for vulnerability disclosure, carries out the following tasks:
a) identifies and contacts relevant entities.
b) assists individuals or legal entities reporting vulnerabilities.
c) negotiates the timelines for the discovery and management of vulnerabilities affecting multiple entities.
3. The national CSIRT, as the coordinator for vulnerability disclosure, ensures that the appropriate actions are taken by information infrastructure operators regarding the reported vulnerability and ensures the anonymity of the reporting entity.
4. When a reported vulnerability affects the information infrastructures of other states, the national CSIRT, when necessary, collaborates with other designated CSIRTs based on an agreement in accordance with applicable legal provisions.
5. The national CSIRT develops and maintains a register of identified vulnerabilities, which contains the following information:
a) description of the vulnerability.
b) affected IT products or services and the severity level in relation to the circumstances in which it may be exploited.
c) guidelines for the provided solutions to mitigate the risks arising from the discovered vulnerabilities.

Article 15
Sectoral CSIRTs and CSIRTs near operators of information infrastructures

1. Entities responsible for providing services in accordance with the provisions set forth in Article 11 of this law establish their sectoral CSIRT within their structure, responsible for cybersecurity incidents.
2. The operator of critical infrastructure and the operator of important information infrastructure establish within their structure a cybersecurity incident response team, CSIRT.
3. CSIRTs fulfill the requirements as follows:
a) ensure a high level of availability of their communication channels, avoiding any failure to contact or be contacted by other parties at any time, clearly specifying communication channels.
b) have their environments and supporting information systems located in secure places.
c) are equipped with an appropriate system for managing and handling requests, especially to facilitate deliveries to be effective and efficient.

d) ensure the confidentiality and reliability of their operations.
e) have suitable and trained personnel to ensure the availability of their services at all times and can participate in international cooperation networks for this purpose.
f) are equipped with additional compensation systems to ensure the continuity of their services.
4. The technical rules for the operation of CSIRTs near operators of critical and important information infrastructures and sectoral CSIRTs are defined in the regulation approved by order of the General Director of the Authority.
5. The manner of setting up sectoral CSIRTs is determined by the Decision of the Council of Ministers.

Article 16
Tasks of the sectorial CSIRT

The Cybersecurity Incident Response Team for Critical and Significant Information Infrastructures, the sectoral CSIRT, performs the following duties:
a) collaborates with the Authority to identify critical and significant information infrastructures within the Republic of Albania;
b) coordinates with the National CSIRT to enhance the level of cybersecurity within the critical and significant information infrastructures managed by the respective operators, according to their area of activity;
c) assumes responsibility for reporting cybersecurity incidents occurring within the managed critical and significant information infrastructures and by the operators, in accordance with their area of activity;
d) maintains logs of identified or reported incidents for a specified period as regulated by an order approved by the General Director of the Authority;
e) coordinates with the operators of critical and significant information infrastructures for protection against cybersecurity incidents affecting the systems and networks they manage;
f) notifies the National CSIRT immediately upon incident identification, and informs it in the event of a rapid resolution of the incident within the managed infrastructures;
g) provides assistance to the operators of information infrastructures as necessary, and makes available the necessary information that may facilitate effective incident handling;
h) enhances staff capacities through periodic training and certifications according to the sectors they cover;
i) appoints the contact point and reports to the National CSIRT, and notifies any changes within 7 calendar days;
j) cooperates with stakeholders in the private sector, aiming to fulfill the objectives of this law;
k) implements cybersecurity policies at the sectoral level."

Article 17
Responsibilities of the CSIRT to the operators of critical and important information infrastructures

1. The operator of critical information infrastructure shall establish within its organizational structure a Cybersecurity Incident Response Team (CSIRT).
2. The operator of significant information infrastructure shall include within its structure a person responsible for responding to cybersecurity incidents.
3. The CSIRT at the operators shall perform the following duties:
a) Monitor the networks and information systems within their critical or significant information infrastructure for cybersecurity incidents or potential cyber-attacks;
b) Identify and categorize the incident, as well as assess the extent and damage caused by it;
c) Address the incident and provide specific solutions based on the policies and measures defined in this law, and cooperate with relevant law enforcement institutions when elements of cybercrime or other related criminal acts are suspected;
d) Prevent similar incidents in the future by taking preventative measures;
e) Prepare and submit incident reports to the National CSIRT in accordance with the format and deadlines specified in this law and the regulations approved by the order of the General Director of the Authority;
f) Maintain logs for a specified period as determined in the regulations approved by the order of the General Director of the Authority;
g) Keep and preserve the chronology of all evidence of the incident in accordance with the provisions of this law and current legislation on personal data protection;
h) Report any cybersecurity incident that occurs within their infrastructures to the National CSIRT and the sectoral CSIRT;
i) Implement cybersecurity policies at the institutional level.

Article 18

Points of contacts

1. Operators of critical and important information infrastructures designate contact points according to the provisions made in this law.
2. Data for contact points for public and private legal entities include:
a) Name;
b) Headquarters address;
c) Identification number (NUIP) of the legal entity or a similar number assigned outside the country, and;
d) Contact person details authorized to act on behalf of the operator, including email address, IP ranges, and phone numbers.
3. Contact points are reported by operators of critical and important information infrastructures to the national CSIRT and sectoral CSIRT within 15 days after the entry into force of the list of critical and important information infrastructures approved by the Decision of the Council of Ministers.

4. Any changes in the contact point information are officially communicated to the national CSIRT and sectoral CSIRT by operators of critical and important information infrastructures within 7 calendar days.

Article 19
Information Sharing

1. Operators of critical and important information infrastructures voluntarily exchange information among themselves regarding cybersecurity threats, vulnerabilities, compromise indicators, techniques and procedures, specific threat actor information, cyber safety signals, and recommendations, as well as the configuration of cybersecurity tools for detecting cyberattacks, with the aim of:
a) Preventing, detecting, responding to cyber incidents, or recovering from and mitigating the impact of cyber incidents;
b) Enhancing the level of cybersecurity, particularly by raising awareness about cybersecurity threats, limiting or impeding the spread of such threats, relying on various protective capacities, vulnerability correction and discovery, detection techniques, incident control and prevention, response, recovery phases, and promoting collaboration between public and private entities concerning the analysis of cyber incidents.
2. Voluntary exchange of information between operators is carried out through agreements for sharing cyber security information while maintaining the confidentiality of the shared information in all cases.
3. Information infrastructure operators, in accordance with the provisions of this article, are obligated to notify the Authority in every case regarding the signing and conclusion of these information sharing agreements.

CHAPTER III
ADMINISTRATION OF CYBER SECURITY

Article 20
Cyber security measures

1. Operators of critical and important information infrastructures are obligated to implement cybersecurity measures and document their implementation according to the provisions made in this law.
2. To ensure service continuity, operators of critical and important information infrastructures implement appropriate and proportionate measures to achieve a high level of cybersecurity in their infrastructures.

3. Cybersecurity measures are classified into organizational, technical, and operational measures for risk management and are adapted by the Authority considering recent technological developments.
4. Cybersecurity measures aim to prevent and minimize the impact of incidents on the security of networks and information systems.
5. The content and documentation method of organizational, technical, and operational cybersecurity measures are determined by a decision of the Council of Ministers.
6. Entities operating in sectors according to the annexes of this law but are not yet part of the list of information infrastructures can apply all cybersecurity measures outlined in this law in advance.

Article 21
Risk management measures for critical and important information infrastructure operators

1. Operators of critical and significant information infrastructure shall implement technical, organizational, and operational measures for risk management, which include:
   a) Establishing policies for incident risk analysis and information system security;
   b) Incident handling;
   c) Continuity of operations, including backup management and recovery, disaster recovery, and crisis management;
   d) Supply chain security, encompassing security aspects related to relationships between each entity and it's direct supplier or service provider;
   e) Security in the procurement, development, and maintenance of information systems and networks, including vulnerability management and detection;
   f) Policies and procedures for assessing the effectiveness of cybersecurity risk management measures;
   g) Basic cybersecurity hygiene practices and cybersecurity training;
   h) Policies and procedures concerning the use of cryptography and, where applicable, encryption;
   i) Human resource security, access control policies, and asset management;
   j) The use of multi-factor authentication or continuous verification solutions, secure voice, video, and text communications, and secure emergency communication systems within the entity, as appropriate.
2. In implementing organizational, technical, and operational risk management measures, operators particularly consider:
   a) The security of networks and service systems;
   b) Incident management;
   c) The management of service continuity and disaster recovery;
   d) Monitoring, auditing, and testing;
   e) Compliance with international standards.

Article 22
Cybersecurity measures in the event of a cyber threat or cybersecurity incident

1. In the event of a cyber incident or potential challenge, cybersecurity measures of the following categories shall apply:
a) Warning measures.
b) Countermeasures and playbooks.
c) Protective measures of a general nature.
2. Warning measures are recommendatory in nature, issued by the Authority in instances of an occurring threat and made available to operators for immediate implementation. These measures are drafted by the Authority and approved by order of the General Director of the Authority.
3. Countermeasures are developed by the Authority and undertaken by operators of critical and significant information infrastructures in response to incidents within their infrastructures. The Authority drafts *playbooks* based on the cybersecurity incident categories of ENISA, which are applied as appropriate to the presented cybersecurity incident. The responsible person, acting as the contact point, immediately informs the Authority about the implementation of countermeasures, *playbooks*, and their outcomes. The approval and implementation of countermeasures and *playbooks* occur by order of the General Director of the Authority.
4. General nature protective measures are based on an analysis of resolved cybersecurity incidents, aimed at enhancing the protection of information networks and systems, and are implemented by operators of critical and significant information infrastructures. These measures are defined in the regulations approved by order of the General Director of the Authority.

Article 23
Cyber security risks and reporting of cyber security incidents

1. Operators of critical and significant information infrastructures shall take measures to prevent and minimize the impact of cybersecurity risks and incidents on their information infrastructures.
2. Operators of critical and significant information infrastructures collaborate with the National CSIRT and the sectoral CSIRT at all stages of a cybersecurity incident occurring within their information infrastructures.
3. Operators of critical and significant information infrastructures report all types of cybersecurity incidents to the National CSIRT and the sectoral CSIRT within 4 hours from the identification of the incident. In the case of significant incidents, within 72 hours from the identification of the significant incident, operators update the information and make an initial assessment of the significant incident, including severity and impact, as well as, where present, indicators of compromise.
4. To determine the significance of the impact of a cybersecurity incident, the following parameters are evaluated:
   a) The number of users affected by the service disruption;
   b) The duration of the incident;
   c) The geographic extent regarding the area affected by the incident;

d) The degree of disruption to service functioning;
e) The extent of impact on economic and social activities;
f) The dependency of sectors on the services provided by the information infrastructure operator;
g) The importance of maintaining an adequate level of service, considering the availability of alternative means to provide this service.

5. Within one month after notifying the incident, according to point 3 of this article, operators of critical and significant information infrastructures shall submit a final report to the National CSIRT, which contains:

a) A detailed description of the incident, including its significance and impact;
b) The type of threat or the main cause that may have caused the incident;
c) Implemented measures and ongoing measures for mitigating the consequences;
d) Where applicable, the cross-border impact of the incident.

6. In cases of an ongoing cybersecurity incident, the affected information infrastructure operator, in addition to the obligation to submit the final report according to point 5 of this article, has the duty to submit a progress report to the National CSIRT at the time of the cybersecurity incident occurrence.

7. The Authority makes available to international organizations in the field of cybersecurity the data managed related to cybersecurity incidents, aiming for their handling and resolution. Communication and data sharing according to the provisions of this point are carried out in accordance with current legislation on international agreements and personal data protection.

8. The types and categories of cybersecurity incidents affecting information systems and networks, the reporting format, reporting elements, reporting deadlines, the method of documenting, and registering cybersecurity incidents are determined by the regulations approved by order of the General Director of the Authority.

Article 24
Additional Cybersecurity Measures

Operators of critical information infrastructures, in addition to the cybersecurity measures provided for in Articles 21 and 22 of this law, may adopt additional risk management or cybersecurity incident reporting measures that are in accordance with European Union regulatory acts and do not contradict the provisions set forth in this law.

Article 25
Voluntary Reporting of Cybersecurity Incidents

1. In addition to the operators of critical and significant information infrastructures, other entities also voluntarily report.

2. The National CSIRT examines the reports made and, depending on them, determines the significance of the impact of the cybersecurity incident according to the parameters mentioned in point 4 of Article 23 of this law, applying the principle of confidentiality in every case.

3. Voluntary reports are considered by the Authority only after it has been assessed that these reports do not affect the handling of mandatory reports from operators of critical and significant information infrastructures.
4. Voluntary reporting does not create consequences or obligations for the reporting entity if it would not have made such a report.

Article 26
Public and User Information on Cyber Incidents

1. After consulting with the information infrastructure operator, the National CSIRT informs the public about incidents occurring in critical and significant information infrastructures when such notification is necessary for public awareness, to prevent a significant incident, to handle the incident, or when it concerns public interest, or it requires the information infrastructure operator to do so while maintaining the confidentiality of the incident data.
2. Public notification is carried out according to a communication procedure approved by order of the General Director of the Authority.
3. Operators of critical and significant information infrastructures promptly notify their service users potentially affected by a significant cybersecurity incident about measures those users can take in response to that threat.
4. A cybersecurity incident is considered significant if:
a) It has caused or is capable of causing severe operational disruptions to services or financial loss to the affected operator;
b) It has impacted or is capable of affecting other natural or legal persons, causing substantial material or immaterial damage.
5. If a reported cybersecurity incident affects one or more other states, the National CSIRT notifies the affected states in accordance with the provisions of this law and the current legislation on personal data protection.

Article 27
Data Limitation and Confidentiality Preservation

1. Authority officials involved in resolving the cyber incident are obliged to maintain complete confidentiality for all data processed during the resolution procedure.
2. Data confidentiality is preserved even after the termination of employment with the Authority in accordance with current legal provisions.
3. The confidentiality of cyber incident data is treated according to current legislation on classified information and legislation on personal data protection.

Article 28
Cyber Crisis

1. In cases where it is impossible for the responsible cybersecurity entities to avert a cybersecurity threat towards networks and information systems, the Authority, in coordination with other responsible security and defense entities as specified in Article 11(a) of this law, immediately

proposes to the Prime Minister the declaration of a cybersecurity crisis state and emergency measures for resolving the situation.
2. The state of cybersecurity crisis is declared by a decision of the Council of Ministers, upon the proposal of the Prime Minister. The decision to declare a state of cybersecurity crisis is announced in the media.
3. The state of cybersecurity crisis is declared for a period of up to 7 days. This period may be extended repeatedly, depending on the complexity of the cybersecurity situation, by a decision of the Council of Ministers. The maximum period for declaring a state of cybersecurity crisis shall not exceed 30 days.
4. During the period of the cybersecurity crisis state, the General Director of the Authority informs the Prime Minister about the progress and resolution of this state, as well as about potential real threats.
5. During the state of cybersecurity crisis, the Authority coordinates crisis management and has the right to issue general decisions or take general protective measures and countermeasures.
6. Countermeasures issued by the Authority before the declaration of the cybersecurity crisis state remain in effect as long as these countermeasures do not conflict with the emergency measures declared by the Council of Ministers.
7. The Authority coordinates the actions of all responsible structures for resolving the cybersecurity crisis state.
8. In accordance with the above provisions, the Authority approves a national plan for response to widespread cybersecurity incidents and cybersecurity crises, which specifies:
a) Objectives and preparedness measures at the national level, as well as activities;
b) Duties and responsibilities of entities responsible for managing the cybersecurity crisis;
c) Cybersecurity crisis management procedures, including their integration into the national legal framework for general cybersecurity crisis management, as well as information exchange channels;
d) National preparedness measures, including exercises and training activities;
e) Relevant public and private parties, as well as involved infrastructures;
f) National procedures and agreements between the Authority and relevant national bodies to ensure effective participation and support in the coordinated management of cybersecurity incidents and widespread cybersecurity crises at the national level.
9. Procedures for identifying, classifying, escalating, and managing the cybersecurity crisis are determined by a decision of the Council of Ministers.

Article 29
Cybersecurity Emergency and Crisis Response Team – CERT

1. For the timely and efficient handling of emergencies and the cybersecurity crisis, in accordance with the provisions of this law, an ad-hoc structure, on a case-by-case basis, called the "cybersecurity emergency response team – CERT," is established within the Authority.

2. The CERT consists of field experts, who are called upon by the Authority for the drafting of the emergency measures plan, management, and resolution of emergencies and the cybersecurity crisis.
3. The CERT, in the exercise of its duties, is obliged to respect the principle of confidentiality.
4. The establishment, organization, and operation of the CERT are determined by a decision of the Council of Ministers.

CHAPTER IV
MONITORING AND ENFORCEMENT OF CYBER SECURITY MEASURES

Article 30
Supervision and Implementation of Cybersecurity Measures

The Authority oversees the implementation of cybersecurity measures by operators of critical and significant information infrastructures.
In the exercise of its supervisory activities, the Authority exercises the following powers:
a) Monitors operators through periodic inspections, as well as whenever deemed reasonable, in each case, notifying the operator 10 working days prior to the inspection;
b) Conducts inspections of declared networks and systems, as well as any other or interconnected networks or systems, through an annual inspection plan developed at the beginning of each year, which is approved by order of the General Director of the Authority and published on the official website of the Authority;
c) Carries out inspections with ad-hoc groups in cases of a cybersecurity incident occurrence or potential breaches of this law;
d) Performs external scans of operators' networks and systems for the purpose of verifying security measures related to potential vulnerabilities, in each case, by informing the information infrastructure operator in advance, ensuring process transparency and guaranteeing the confidentiality of information;
e) Requests the necessary information to assess the security level of information networks and systems to access the risk management measures taken by operators;
f) Collects data, documents, and necessary information to perform its supervisory function over operators, informing critical and significant information infrastructure operators in advance and ensuring the protection of this information;
g) Requests and verifies documented records for the effective implementation of cybersecurity policies as part of the inspection process.

Article 31
Obligations of Operators of Critical and Significant Information Infrastructures

1. Operators of critical and significant information infrastructures are obligated to report all their critical and significant infrastructures, as well as any other infrastructures that interact with them, to the Authority.

2. Operators of critical and significant information infrastructures are required to continuously report to the Authority any new infrastructure administered by them that interacts with categorized critical or significant infrastructures.
3. Operators of critical and significant information infrastructures are obliged to document any changes and developments made in their critical and significant infrastructures.
4. Operators of critical and significant information infrastructures are obligated to provide the Authority with any documentation and evidence requested by the Authority as part of the inspection process.
5. Operators of critical and significant information infrastructures, as part of the supervisory activity, provide direct access to their information environments and systems to the National CSIRT, in accordance with the security procedures of each operator of these infrastructures, which are related to the services they offer.
6. Operators of critical and significant information infrastructures are required to implement corrective measures issued by the Authority and report on their implementation.
7. For the effective implementation of cybersecurity measures, operators submit to the Authority a conformity assessment report from a conformity assessment body for cybersecurity at least once every 2 years.
8. Operators of critical and significant information infrastructures are required to take additional technical measures, in accordance with the decisions made by the Council of Ministers, regarding the content and documentation of cybersecurity measures.
9. Operators of critical and significant information infrastructures are obliged to cooperate with the Authority in carrying out the supervisory functions defined in this law.

Article 32
Other Obligations of Operators of Critical and Significant Information Infrastructures of the Public Administration

1. Operators of critical and significant information infrastructures of the public administration as per annex 1 of this law, with the aim of ensuring the establishment of security and interoperability standards with government systems, before initiating the implementation of a system, must obtain confirmation from the responsible institution according to the current legislation on e-governance related to technical specifications as defined in the current public procurement law.
2. Operators of critical and significant information infrastructures of the public administration as per annex 1 of this law, host the primary node of their infrastructure at the Government Data Center and the secondary node at the Business Continuity Center.
3. Operators of critical and significant information infrastructures of the public administration as per annex 1 of this law, are monitored by the National Cybersecurity Center.

CHAPTER V
COOPERATION AT NATIONAL AND INTERNATIONAL LEVEL

Article 33

National Level Cooperation

1. The Authority coordinates its activities with security and defense institutions and cooperates with other entities responsible for cybersecurity in accordance with the provisions of this law.
2. CSIRTs within operators, sectoral CSIRTs are obliged to always cooperate with the National CSIRT and the Authority, in fulfillment of the duties and responsibilities arising from this law.
3. In accordance with paragraph 1 of this article, the Authority:

a) cooperates with the State Police and relevant institutions in cases where, based on the information obtained under this law, there are suspicions of elements of cybercrime, or other criminal offenses related to it;

b) cooperates with the institution responsible for classified information security in cases where it becomes aware of possible threats to classified networks, information infrastructures, subject to this law;

c) cooperates with the institution responsible for electronic and postal communications, AKEP, for the security of networks and electronic communication services as well as for the closure of websites with illegal content and IPs that generate attacks, malware;

d) cooperates with the national authority for the protection of personal data, in cases where incidents in information infrastructures result in the illegal dissemination of personal data.

Article 34
International Cooperation

1. The Authority cooperates with international organizations in the field of cybersecurity and national authorities of other countries, through mutual agreements, in accordance with the current legislation on international agreements.
2. In fulfilling commitments in terms of cybersecurity as a member of the North Atlantic Treaty Organization (NATO) and the Organization for Security and Co-operation in Europe (OSCE), the Authority coordinates and harmonizes work between these organizations and national institutions.
3. The Authority cooperates with the Cooperation Group, the CSIRT Network, the European Network of Crisis Management Organizations (EU-CyCLONe) in accordance with the provisions of this law.
4. The Authority participates in international forums on cybersecurity issues and collaborates with them to enhance cybersecurity in the country.

Article 35
Cooperation Group

The Authority participates in the activities of the Cooperation Group composed of representatives from the Member States of the European Union, the European Commission, and the European Union Agency for Network and Information Security (ENISA), primarily contributing to:

a) The exchange of information and best practices concerning:

i. Cyber threats and cybersecurity incidents;
ii. Vulnerabilities;
iii. Training and capacity building;

iv. Awareness in the field of cybersecurity;
v. Standards and technical specifications;
vi. Identification of critical and important information operators;
vii. New policy initiatives on cybersecurity and specific sector requirements for cybersecurity;
viii. The implementation of EU-specific sectoral legal acts containing provisions on cybersecurity;
b) The assessment of the supply chain risk process at the EU level related to ICT services, ICT systems, and ICT products.
c) Cases of mutual assistance, including experiences, outcomes, and joint cross-border actions;
d) Policies for follow-up actions after cybersecurity incidents and crises on a wide scale based on lessons learned from the CSIRTs network and EU-CyCLONe;
e) Reviewing the level of cybersecurity according to the provisions made in Article 38 of this law.

Article 36
CSIRTs Network

The National CSIRT participates in the CSIRTs Network, primarily contributing to:
a) The exchange of information and best practices on CSIRTs capabilities;
b) Cybersecurity incidents, cyber threats, risks, and vulnerabilities;
c) Providing assistance in handling cross-border incidents;
d) Forms of operational cooperation, including:
i. Categories of cyber threats and incidents;
ii. Warnings;
iii. Mutual assistance;
iv. Principles and agreements for coordination in response to cross-border risks and incidents;
v. Contribution to the national cybersecurity incident on a wide scale and the cyber crisis response plan, at the request of a Member State;
e) Cooperation and information exchange with Security Operations Centers (SOCs), at the national and European Union level, for joint situation awareness on cybersecurity incidents and threats.

Article 37
European Network of Cyber Crisis Liaison Organizations (EU-CyCLONe)

The Authority participates with the European Network of Cyber Crisis Liaison Organizations (EU-CyCLONe) in managing cybersecurity incidents and crises on a wide scale, primarily contributing to:
a) Enhancing the readiness level for managing cybersecurity incidents and crises on a wide scale;
b) Joint situation awareness for cybersecurity incidents and crises on a wide scale;
c) Assessing the consequences and impact of cybersecurity incidents and crises on a wide scale and proposing mitigating measures;
d) Coordinating the management of cybersecurity incidents and crises on a wide scale;
e) Providing assistance upon the request of an interested Member State, in cases of national cybersecurity incidents on a wide scale and cyber crisis response plans.

Article 38
Review of Cybersecurity at the European Union Level

The Authority participates in the review of the cybersecurity level through cybersecurity experts regarding:
a) The level of implementation of cybersecurity risk management measures and obligations according to the provisions made in this law;
b) The level of capabilities including available financial, technical, and human resources and the effectiveness of the exercise of the duties of competent authorities;
c) The operational capabilities of CSIRTs;
d) The level of implementation of mutual assistance according to the provisions made in this law;
e) The level of implementation of agreements for sharing cybersecurity information according to the provisions made in this law;
f) Specific issues of a cross-border or cross-sectoral nature.

CHAPTER VI

CYBER SECURITY CERTIFICATION

Article 39
Preparation, review and approval of a national cyber security certification scheme

1. The authority prepares the national cyber security certification scheme in accordance with the approved schemes of the European Union for Cyber Security Certification.
2. For the preparation of the national cyber security certification scheme, the Authority consults with interest groups, through a formal, open, transparent and comprehensive consultation process.
3. At least every five years, the Authority evaluates the approved cyber security certification schemes, taking into consideration the suggestions of interested parties.
4. The authority publishes on the website in the dedicated menu the national cyber security certification schemes, cyber security certificates, as well as information about the schemes that are no longer valid or abolished.
5. A year after the entry into force of the cybersecurity certification scheme, the Authority publishes the list of accredited Conformity Assessment Bodies for Cybersecurity according to the cybersecurity certification scheme.

Article 40
The security objectives of the national scheme of cyber security certification

A national cyber security certification scheme fulfils, as the case may be, at least the following security objectives:
a) protection of stored, transmitted, or processed data, against accidental or unauthorized disclosure, throughout the life cycle of the ICT product, service, or process.

b) protection of stored, transmitted, or processed data against accidental or unauthorized destruction, loss, alteration, or lack of availability throughout the life cycle of the ICT product, service, or process.
c) authorization of persons, programs, or machines, only on access to data, services or functions to which their access rights refer.
d) identification and documentation of established vulnerabilities.
e) recording of data, services, or functions, which have been accessed, used or processed, including time and individual.
f) to enable control over which data, services or functions are accessed, used, or processed, including timing and authorship.
g) verification that ICT products, services and processes do not contain known vulnerabilities
h) restore availability and access to data, services, and functions in a timely manner, in the event of a physical or technical incident.
i) ICT products, services and processes are secure by design.
j) ICT products, services and processes are equipped with up-to-date software and hardware, which do not contain known vulnerabilities and are equipped with secure update mechanisms.

Article 41
Certification of specific ICT products, services and processes

1. Operators of critical and important information infrastructures utilize products, services, and ICT processes developed either internally or offered by third parties, certified according to the National Cybersecurity Certification Scheme or a European Cybersecurity Certification Scheme.
2. To increase the level of cyber security in information infrastructures, the Authority encourages operators to use electronic identification and qualified trusted services, according to the legal framework in force for them.

Article 42
Approval of schemes, levels, and bodies responsible for cyber security certification

1. Determined by a decision of the Council of Ministers:
a) National cyber security certification scheme, in accordance with the Certification Schemes approved by the European Union, as well as the deadlines related to the implementation of the cyber security certification scheme by the subjects of this law;
b) Security levels of the national cybersecurity certification scheme for ICT products, services, and processes.
2. The procedure and criteria for registering Conformity Assessment Bodies for Cybersecurity under the Cybersecurity Certification Scheme are defined by guidance from the Director General of the Authority.
3. The Council of Ministers approves the registration fee amount that Conformity Assessment Bodies for Cybersecurity must pay to the Authority, in compliance with the obligations specified in this law.
4. The revenues derived from the registration fee shall be deposited into the State Budget.

CHAPTER VII

ADMINISTRATIVE MEASURES

Article 43

Corrective Measures

1. When the Authority finds deficiencies in the implementation of cybersecurity measures, pursuant to this law, it shall set a reasonable deadline within which critical and important information infrastructure operators shall take appropriate corrective measures.

2. When the Authority finds that critical and important information infrastructure operators have not complied with the obligation specified in Article 31(2) of this law, it shall set a reasonable deadline within which operators shall take measures to fulfill the obligation.

3. The costs related to the implementation of corrective measures shall be borne by critical and important information infrastructure operators.

4. Operators are obliged to notify the Authority of the implementation of corrective measures within the specified deadline and to provide supporting documentation on these measures.

5. The categorization of deadlines according to the type and identified deficiencies as stipulated in paragraphs 1 and 2 of this article shall be determined in the decision of the Council of Ministers on the content and manner of documenting cybersecurity measures pursuant to Article 20 of this law.

Article 44

Administrative Offenses

Under the terms of this law, the following violations constitute administrative offenses:
a) Failure to report a cybersecurity incident that occurred in infrastructures to the National CSIRT and the sectoral CSIRT, as defined in item "ë" of point 3 of Article 17 and point 3 of Article 23 of this law;
b) Inaccurate reporting of information infrastructures during the identification process, according to the provisions of point 4 of Article 12 of this law and subordinate acts in its implementation;
c) Failure to report to the Authority the contact point or their updates, according to the provisions in points 3 and 4 of Article 18 of this law;
d) Non-compliance with obligations set by the Authority, in implementation of point 1 of Article 27 of this law;
e) Non-fulfillment of obligations by operators, as defined in points 1, 3, 4, 5, 7, 8, and 9 of Article 31 of this law;
f) Non-fulfillment of obligations by operators, in implementation of points 1, 2, 4 of Article 43 of this law;
g) Non-fulfillment of obligations, as specified in points 5 and 6 of Article 23 of this law;
h) Non-fulfillment of obligations specified in points 1 and 2 of Article 32 of this law.

Article 45
Administrative Sanctions

1. When the Authority identifies a violation of provisions constituting an administrative offense, as per Article 44 of this law, it imposes a fine as follows:
a) From 1,000,000 to 10,000,000 Albanian lekë for administrative violations specified in items "a" and "e" of Article 44 of this law;
b) From 200,000 to 400,000 Albanian lekë for administrative violations specified in items "b", "c", "d", and "g" of Article 44 of this law;
c) From 400,000 lekë to 1,000,000 lekë for administrative violations specified in item "f" of Article 44 of this law;
d) From 2,000,000 lekë to 5,000,000 lekë for administrative violations specified in item "h" of Article 44 of this law.
2. The methodology for determining the amount of the administrative fine is defined by an order of the General Director of the Authority.
3. Revenues generated from administrative offenses are allocated 100 percent to the state budget.

Article 46

Suspension of Service Provision

1. When the Authority identifies repeated violations regarding the implementation of cybersecurity measures defined in this law by the operator of critical information infrastructure, against whom up to 2 consecutive administrative measures have been taken for non-compliance with obligations arising from this law, it simultaneously has the right:
a) To submit a request to the competent institution for blocking the domain/subdomain associated with the service;
b) To submit a request to the competent institution for licensing, certification, or authorization of the relevant service for temporary suspension of the license, authorization, or permission to operate the service for which deficiencies in implementing security measures have been identified;
c) To submit a request to the competent institution for temporary suspension of the executive director or legal representative who is responsible for management in critical infrastructures.
2. When measures specified in items "a", "b", or "c" of point 1 of this article have been taken against the operator of critical infrastructure, these measures continue to be applied until the operator undertakes the necessary actions to correct the deficiencies or fulfill the requirements for which these measures were imposed.
3. When the operator has taken measures to remedy the deficiencies or requirements identified for which measures specified in items "a", "b", or "c" of point 1 of this article were given, the Authority requests the competent institution to remove them.

Article 47

Procedure for Imposing Administrative Fines

The procedures for establishing, examining, appealing, and executing administrative offenses are those provided for in the current law on administrative offenses.

CHAPTER VIII

Article 48

Subordinate Legislation

1. The Council of Ministers is charged with adopting subordinate acts within 6 months from the entry into force of this law in implementation of Articles 7, points 7, 9, item "ë", 12, point 2, and 20, point 5, of this law.
2. The Council of Ministers is charged with adopting the National Cybersecurity Strategy within 9 months from the entry into force of this law in implementation of Article 6, points 4 and 5, of this law.
3. The Council of Ministers is charged with adopting subordinate acts within 9 months from the entry into force of this law in implementation of Articles 28, point 9, and 29, point 4, of this law.
4. The General Director of the Authority is charged with issuing subordinate acts within 6 months from the entry into force of this law in implementation of Articles 13, item "f", 15, point 4, 22, point 4, 23, point 8, and 45, point 2, of this law.
5. The General Director of the Authority is charged with issuing a subordinate act within 9 months from the entry into force of this law in implementation of item "k" of Article 13 of this law.
6. The General Director of the Authority is charged with issuing a subordinate act within 12 months from the entry into force of this law in implementation of item "gj" of Article 13 of this law.
7. The General Director of the Authority is charged with approving the corresponding playbooks within 12 months from the entry into force of this law in implementation of point 3 of Article 22 of this law.
8. The Council of Ministers is charged with adopting the method for establishing sectoral CSIRTs within 12 months from the entry into force of this law in implementation of point 5 of Article 15 of this law.
9. The Council of Ministers is charged with adopting the subordinate acts specified in items "a" and "b" of point 1 of Article 42 of this law within 12 months from the approval of the European cybersecurity certification scheme.
10. The Council of Ministers is charged with adopting a subordinate act in implementation of point 3 of Article 42 of this law within 6 months from the approval of the cybersecurity certification scheme.
11. The General Director of the Authority is charged with issuing a subordinate act in implementation of point 2 of Article 42 of this law within 6 months from the approval of the cybersecurity certification scheme.

Article 49

Repeals

1. Law no. 2/2017 "On Cybersecurity" is repealed.
2. Articles 10, 10/1 of law no. 9880/2008 "On Electronic Signature" as amended are repealed.
3. Subordinate legislation adopted pursuant to law no. 2/2017 "On Cybersecurity" remains in force even after its repeal when not in conflict with the provisions of this law, until the adoption of subordinate legislation pursuant to this law.

Article 50
Transitional Provisions

1. Entities responsible in the field of cybersecurity are obligated to align their activities with the provisions of this law within 24 months from the date of its entry into force.
2. The National Authority for Electronic Certification and Cybersecurity continues to operate as the responsible institution in the field of cybersecurity until its reorganization in accordance with the provisions of this law.
3. The National Cybersecurity Authority, following the entry into force of this law, will also continue to exercise its powers according to the definitions made in Law No. 9880, dated 25.2.2008, "On electronic signature," as amended, and in Law No. 107/2015 "On electronic identification and trust services," as amended, until the entry into force of the new law on electronic identification and trust services.
4. The obligations envisaged for the National CSIRT, according to this law, also apply to reporting to the responsible EU bodies in the case of the Republic of Albania's membership in the European Union.
5. Upon the entry into force of this law and every two years thereafter, the Authority, as the single national contact point, sends the necessary information for the implementation of this law to the European Commission and ENISA, especially regarding the identification of operators of critical and significant information infrastructures, in compliance with the law on personal data protection for international transfer.
6. In the case of the Republic of Albania's membership in the European Union, the Authority reports to the European Commission and ENISA once a year on the types of incidents that have occurred in the Republic of Albania.
7. With the Republic of Albania's membership in the European Union, the Authority notifies the European Commission of any cybersecurity certification scheme, for cybersecurity conformity assessment bodies that have been accredited, as well as any subsequent changes.

Article 51
Entry into Force

1. This law shall enter into force 15 days after its publication in the Official Gazette.
2. Articles 35, 36, 37, and 38 shall come into effect upon the Republic of Albania's accession to the European Union.

Approved on 21.3.2024.

Promulgated by decree no. 149, dated 16.4.2024, from the President of the Republic of Albania,
Bajram Begaj.

Annex 1
High Critical Sectors.

Sector	Sub-sector	Subject type
Energy	**Electricity**	• Electricity companies • Distribution system operators • Manufacturers • Designated electricity market operators • Market participants, natural or legal persons who buy, sell or produce electricity • Operators of a top-up point who are responsible for the management and operation of a top-up point, which provides a top-up service to end-users, including on behalf of and on behalf of a mobile service provider
	Central heating and cooling	• Operators of Central heating and cooling
	Oil	• Oil transmission pipeline operators • Operators of oil production, processing and handling, storage and transmission facilities • Central subjects
	Gas	• Supply companies • Distribution system operators • Transmission system operators • Storage system operators • Liquefied natural gas system operators • Natural gas companies • Operators of natural gas processing and treatment facilities

	Hydrogen	• Operators of hydrogen production, storage, and transmission
Transportation	**Air**	• Air carriers for commercial reasons • Airport management entities • Traffic management control operators providing air traffic control
	Railway	• Infrastructure managers • Railway undertakings, including operators of service facilities
	Maritime	- Inland, maritime and coastal water transport companies for passengers and goods, o excluding individual vessels operated by these companies - Port management bodies, including their port facilities and entities operating works andthe devices included within the ports - Vessel Traffic Services (VTS) Operators
	Road	• Road authorities responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their overall activity • Operators of Intelligent Transport Systems
Banking		Credit Institutions
Financial Market Infrastructure		Financial Market Operators Central Counterparties (operators of financial market infrastructures)
Health		• Health care providers • Entities that carry out research and development activities of medicinal products • Manufacturing entities of basic pharmaceutical products and pharmaceutical preparations • Entities that produce medical devices that are considered critical during a public health emergency (list of critical public health emergency devices)
Entities that provide services or host systems for the processing and transmission of		• State Police • Entities providing services in sectors for the processing and transmission of classified information related to public security

classified information related to public security.		
Drinking Water Supply		• Suppliers and distributors of water intended for human consumption
Wastewater		• Enterprises that collect, dispose or treat urban sewage, domestic sewage or industrial waste, excluding enterprises for which the collection, disposal or treatment of urban sewage, domestic sewage or industrial waste is a non-essential part of their overall activity
Digital infrastructures	**Electronic and communication services**	• Internet Exchange Point providers • DNS service providers, excluding operators of root name servers (root name servers) • Operators of TLD name registries • Cloud computing service providers • Data center service providers • Content delivery network providers • Trusted service providers • Providers of public electronic communications networks • Providers of publicly available electronic communications services
Management of ICT services (business to business)		• Managed service providers • Managed security service providers • Online market providers • Internet search engine providers
Local Public Administration		• Central Government Public Administration Entities • Regional Government Public Administration Entities • Independent Institutions
Space		• Operators of terrestrial infrastructure, owned, managed, and operated by public/private entities, supporting the provision of space-based services, excluding providers of public electronic communications networks
Academic sector		• Entities that provide services in the academic sector.
Tourism		• Entities that provide services in the tourism sector

Annex 2

Other critical sectors

Sector	Sub-Sector	Type of entity
Postal and courier services		• Entities that provide postal services, including courier service providers
Waste Management		• Entities that perform waste management
Chemical Production, Processing, and Distribution		• Enterprises engaged in the production of substances and the distribution of substances or mixtures.
Food production, processing and distribution		• Entities providing services related to logistics and wholesale distribution, as well as large-scale industrial food production and processing.
Production	**Medical Device Production**	• Entities manufacturing medical devices, in vitro diagnostic medical devices, excluding entities producing medical devices mentioned in Annex I, "healthcare" sector.
	Computer, Electronic, and Optical Product Manufacturing	• Enterprises engaged in any of the economic activities referred to for the production of computer, electronic, and optical products.
	Electrical Equipment Manufacturing	• Enterprises engaged in any of the economic activities referred to for the production of electrical equipment.
	Machinery and Equipment Manufacturing n.e.c.	• Enterprises engaged in any of the economic activities referred to in the production of motor vehicles, trailers, and semi-trailers.
	Other Transport Equipment Manufacturing	• Enterprises engaged in any of the economic activities referred to in the production of other transport equipment.
Digital Service Providers		• Online marketplace providers • Internet search engine providers • Social network service platform providers