LAW NO 2/2017

ON CYBERSECURITY

In support of Articles 78 and 83 paragraph 1 of the Constitution, with the proposal of the Council of Ministers,

ASSEMBLY

OF THE REPUBLIC OF ALBANIA

DECIDED:

CHAPTER I
GENERAL PROVISIONS

Article 1

The purpose of the law

The purpose of this law is to achieve a high level of cyber security by defining security measures, rights, obligations and mutual cooperation between the entities operating in the field of cyber security

Article 2

Scope of Application

1. This law applies to communication networks and information systems violation or destruction of which would have an impact on health, safety, economic well-being of citizens, and the effective functioning of the economy in the Republic of Albania.

2. Excluded from the application of this law are the electronic communications networks and information systems that are subject to legal regulations in force for electronic signature, electronic identification and trusted services, electronic communications networks and information systems that process, archive or transmit information classified state information, which are regulated by Law no. 8457, dated 11.02.1999 "On information classified "state secret", as well as electronic communication networks and information systems to the extent provided for in the legislation on electronic communications in the Republic of Albania.

Article 3

Definitions

In this law, the following terms have these meanings:

1. "Responsible Authority for Electronic Certification and Cyber Security", at the following Authority, is the responsible institution, established under the legislation in force for electronic signature.

2. "CSIRT" is the Computer Security Incident Response Team.

3. "Cyber Space" means the digital environment capable of creating, processing and processing exchange information generated by systems, information society services, as well and electronic communication networks.

4. "Cyber Security Incident" is a cyber security event during which there is a violation of the security of services or information systems and networks communication and brings a real negative effect.

5. "Important Information Infrastructure" is the entirety of networks and systems information owned by a public authority, which is not part of the infrastructure critical information, but that could jeopardize or limit the work of the administration public in the event of information security breaches.

6. "Critical Information Infrastructure" is the entirety of networks and systems information, the violation or destruction of which would have a serious impact on health, security and / or economic well-being of citizens and / or the effective functioning of economy in the Republic of Albania.

7. "Responsible Minister" means the Minister in the field of his activity issues information and communication technology.

8. "Critical Information Infrastructure Operator" shall mean a legal person, public or private private sector, which administers critical information infrastructure.

9. "Important Information Infrastructure Operator" is a legal entity public, which administers important information infrastructure.

10. "Cyber Security Risk" is a circumstance or event, identifiable in reasonable way, which can cause the security of the service or security information systems and communication networks.

11. "Communication network and information system" means:

a) an electronic communications network, within the meaning of point 36 of Article 3 of Law no.
9918, dated 19.5.2008, "On electronic communications in the Republic of Albania", of change ";
b. any connected or interconnected equipment or set, of which one or more
that one, based on a program, perform automatic data processing; or
c) digital data stored, processed, found or transmitted by
the elements provided for in points (a) and (b) of this paragraph for the purpose of operation, use, protection and maintenance.

12. "Information Security" is the provision of confidentiality, integrity and confidentiality availability of information.

13. "Cyber Security" means all legal, organizational, technical and legal remedies educational, in order to protect the cyber space.

Article 4

Processing of personal data

Processing of personal data, for the purpose of implementing this law, must be performed on in compliance with the provisions of law no. 9887, dated 10 March 2008, "On Data Protection personal ", as amended.

CHAPTER II
RESPONSIBLE ENTITIES IN THE FIELD OF CYBERSECURITY

Article 5

Responsibilities of Responsible Authority in the field of cyber security

1. The responsible Authority has these powers in the field of cyber security:

a) defines cyber-security measures;

b) acts as the central point of contact at the national level for responsible operators in the field of cyber security and coordinates works for resolving cyber security incidents;

c) administers incident reports in the field of cyber security and ensures the preservation of their registration;

ç) provides help and methodical support to operators responsible in the field of cyber security;

d) performs analysis on the weaknesses found in the field of Internet security,

dh) conducts awareness and education activities in the field of cyber security;

e) acts as the national CSIRT's.

2. The Authority coordinates its activities with the security institutions and collaborates with sectorial CSIRTs and international authorities in the field of cyber security.

Article 6

Other entities responsible

1. Other entities responsible in the field of cyber security are:

a) critical information infrastructure operators,

b) critical infrastructure information operators.

2. The Council of Ministers on the proposal of the minister responsible approves the list of critical information infrastructures. This list is updated at least once in two years.

Article 7

CSIRT

1. Teams responding to computer security incidents (CSIRT) consists of specialists in the field of computer security at any operator that manages critical information infrastructure.

2. Operators of important information infrastructures must have at least one person responsible for computer security incidents.

CHAPTER III

CYBER SECURITY ADMINISTRATION

Article 8

Security measures

1. Security measures include the actions to increase the information security in information systems and availability and reliability of services and communication networks in cyberspace.

2. The operators of critical information infrastructure and operators of critical infrastructure information are obliged to implement security measures and to document their implementation.

3. The operators of critical information infrastructure and operators of critical infrastructure information are obliged to implement the requirements of security measures during the implementation of the infrastructure.

Article 9

Types of security measures

1. The entities responsible in the field of cyber security, in charge of implementation of this law, are obligated to implement security measures of organizational and technical nature.

2. Organizational measures are those of:

a) information security management,

b) risk management,

c) security policies,

ç) organizational security,

d) safety requirements for third parties,

dh) asset management,

e) human resources security and people access,

ë) security events and management of cyber security incidents,

f) management of work continuity;

g) control and audit.

3. Technical measures are those of:

a) physical security,

b) protecting the integrity of communications networks,

c) verifying user identity,

ç) access authorization management,

d) the activity of administrators and users,

dh) detection of cyber security events,

e) means of tracking and evaluating cyber security events,

ë) application’s security,

f) cryptographic equipment,

g) security of industrial systems.

4. The Authority stipulates the content and method of documenting of security measures.

Article 10

Events and incidents of cyber security

Operators of critical information infrastructure and operators of critical infrastructure information are obliged to monitor and detect cyber security events in their infrastructure.

Article 11

Reporting cyber security incidents

1. The operators of critical information infrastructure and operators of critical infrastructure information are required to report to the Authority immediately after detecting cyber security incidents.

2. The Authority determines by regulation the types and categories of cyber security incidents, and the elements and format of cyber security incident report.

Article 12

Incident Data storage

1. The Authority maintainand administer the electronic register of cybersecurity incidents, which contains:

a) the incident report,

b) information to identify the system in which the incident occurred,

c) information on the incident source,

d) the procedure of incident settlement and its results.

2. In the management of incidents affecting the operators defined in Article 6, aimed to determine the significance of the incident should be taken into consideration the parameters below:

a) the number of users affected by the incident,

b) the duration of the incident,

c) the geographical extent of the incident if it can be determined,

d) the financial damage, if it can be determined.

3. The Authority, with the request of public authorities, provides the administered data related to a cyber incident, only if the request complies with the purposes of fulfilling their functional duties.

4. The Authority may make available the administered data related to cyber incidents, to organisms performing the authority role in cybersecurity field abroad and other operators operating in cybersecurity field in order to ensure the cyberspace protection.

Article 13

Data confidentiality

1. The Authority officials, who participate in solving cybersecurity incident, are obligated to maintain confidentiality on all the processed data during the procedure of incident settlement. The confidentiality must be maintained even after the end of the employment relationship with the Authority, except of the cases provided by law.

2. The general director of the Authority can remove the obligation of data confidentiality.

3. The responsible minister determines the cases and criteria on which the confidentiality obligation provided in paragraph 2 of this article can be removed.

Article 14

The measures in case of a threat or cyber incident

1. With the measures in case of a threat or cyber incident, are understood the necessary actions in order to protect the information systems or electronic communications networks, or actions aimed to resolve an ascertain cyber security incident.

2. Measures in case of a threat or cyber incident are:

a) warnings,

b) countermeasures,

c) safeguards.

Article 15

The warnings

1. The warning is a recommendation for dealing with threats in cyber security field. If the Authority finds or get informed of a threat in cyber security field, issues the warning.

2. The warning is released to responsible entities in cyber security field, as appropriate. The warnings are also published on the Authority website.

Article 16

The countermeasures

1. The countermeasures are actions aimed to protect from the cyber risk or cyber security incidents or action aimed to resolve an ascertain incident.

2. The countermeasures are taken by public authorities, operators of critical information infrastructure and operators of significant information infrastructure. The responsible person immediately informs the Authority for the countermeasures implementation and their results.

3. The Authority for the implementation of this article, defines the countermeasures in order to resolve cyber security incident and to determine the duties of the responsible person.

Article 17

The protective measures of a general nature

1. The protective measures of a general nature, are measures based on an analysis of cyber security incidents already solved, in order to increase the protection of information systems, or services or electronic communication networks.

2. The operators of critical information infrastructure and operators of significant information infrastructure are obligated to take protective measures of a general nature.

3. The operators of critical information infrastructure and operators of significant information infrastructure are notified for the release of protective measures of a general nature through contact points.

4. The Authority issues regulations for protective measures of a general nature.

Article 18

Contact Points

1. The operators of critical information infrastructure and critical infrastructure operators to designate points of contact information as defined by this law. The data for the contact points include:

a) for legal persons: name, headquarter address, identification number (TIN) of the legal entity or similar number assigned abroad and contact details of the person who is authorized to act on his behalf.

b) for public legal persons: name, address of headquarters, registration number (TIN), and contact details of the person who is authorized to act on his behalf.

2. Changes in the data of contact points are communicated to Authority from the operators of critical information infrastructure and operators of important infrastructure information.

3. The Authority maintains electronic register of contact points with the information specified in paragraph 1 of this Article.

4. Responsible entities specified in section 6 are required to notify the contact details within 3 months of adoption of this law.

CHAPTER IV

CYBER CRISIS SITUATION

Article 19

Cyber crisis

1. The state of cyber crisis is the situation, in which the security of information or security of information systems and electronic communications networks is seriously jeopardized jeopardizing public interest of the Republic of Albania.

2. The state of cyber crisis announced by the Prime Minister on the proposal of the Minister responsible. Order to declare a state of crisis cyber notified the media.

3. The state of cyber-crisis period posted for up to seven days. Given period may be extended repeatedly after the approval of the Prime Minister. The maximum period of declaring a state of cyber crisis must not exceed 30 days.

4. During the period of crisis situation cyber Minister responsible, inform the Prime Minister about resolving this situation as well as real threats that led to the announcement of this state. During a state

of crisis cyber authority has the right to issue a decision or measure of a general nature and countermeasures.

5. When it is impossible to avoid a threat to the security of information or information systems security services or security and integrity of electronic communications networks, Prime Minister responsibility immediately proposes a state of cyber crisis. Countermeasures taken by the Commission before the establishment of the state of cyber crisis remain in force for as long as these countermeasures do not contradict with the emergency measures announced by the government.

6. The Authority coordinates the activities of all state structures for resolving cyber crisis.

CHAPTER V

ADMINISTRATIVE MISDEMEANOR

Article 20

Corrective measures

1. When the Authority finds shortcomings in the implementation of security measures issued pursuant to this law, he requires the person responsible to correct deficiencies found, and random sets necessary measures to eliminate these shortcomings.

2. Costs associated with the implementation of corrective measures covered by the operators of critical information infrastructure and operators of critical infrastructure information.

Article 21

Administrative Offences

1. For the purposes of this law constitute administrative offenses the following violations:

a) omission of cyber incidents in accordance with Article 10, paragraph 1;

b) the failure of certain obligations by the Authority pursuant to article 12 paragraph 1;

c) omission Authority, the point of contact or their updates pursuant to Article 17, paragraph 4;

d) failure of defined within duties of corrective measures under Article 19.

2. The proceeds of Administrative Offences 100% deposited in the state budget.

Article 22

Administrative sanctions

1. When the Authority finds a violation of the provisions, which constitute an administrative offense under Article 20 of this Law, sets the fine as follows:

a) from 200,000 to 800,000 leks in the event of administrative offenses specified in paragraph 1, letters "a" and "d";

b) by në40.000 Lek 20,000 in case of administrative offenses specified in paragraph 1, letter "c".

c) 40,000 200,000 lek to lek in the event of administrative offenses specified in paragraph 1, letter "b".

Article 23

Procedures

The procedure of ascertainment, examination and execution of administrative offenses are those provided in the law on administrative offenses.

Article 24

Bylaws

1. The Council of Ministers to issue regulations pursuant to paragraph 2 of Article 5 of this law.

2.Authority is loaded to publish the exact regulations issued pursuant to paragraph 4 of Article 8, paragraph 2 of Article 10, paragraph 3 of Article 15 and paragraph 4 of Article 16 of this Law.

3. Minister is loaded with responsible to issue bylaws in paragraph 3 of Article 12.

Article 25

Transitional provisions

1. For existing civil servants of the National Agency for Cyber Security legislation provisions to civil servants in case of closure and restructuring of the institution.

2. National Agency for Computer Security, created by Decision no. 766, dated 14.09.2011, the Council of Ministers "On the establishment of the National Agency for Cyber Security ', as amended, will continue to perform its activities until the start of operation of the new authority, created by the law.

3. Means, sources of income, archives, duties and powers of the National Agency for Cyber Security transferred to the new authority established by this law and the law on electronic signatures.

4. Budgets allocated for the National Agency for Cyber Security and National Authority for Electronic Certification, according to the annual budget law, will unite, representing the approved budget of the responsible authority.

Article 26

Entry into force

This law comes into force 15 days after publication in the Official Journal.

HEAD OF THE PARLIAMENT

ILIR META