

DECISION
No. 783, dated 18.12.2024

**ON THE ORGANIZATION AND FUNCTIONING OF THE NATIONAL CYBER
SECURITY AUTHORITY**

Pursuant to Article 100 of the Constitution and Point 7, of Article 7, of Law no. 25/2024, “On Cybersecurity”, upon the proposal of the Prime Minister, the Council of Ministers

DECIDED:

I. GENERAL PROVISIONS

1. The organization and functioning of the National Cyber Security Authority (hereinafter, the Authority) as a legal, public, budgetary entity, with its headquarters in Tirana, under the authority of the Prime Minister.

2. The Authority shall be financed by the state budget and other lawful sources, in accordance with the applicable legislation on the management of the budgetary system in the Republic of Albania.

3. The mission of the Authority shall be to ensure a high level of cybersecurity for networks and information systems in the Republic of Albania, as well as to guarantee security and reliability in the use of electronic signatures, electronic identification, and trust services.

**II. FUNCTIONAL RESPONSIBILITIES OF THE NATIONAL CYBER SECURITY
AUTHORITY**

1. The Authority shall perform its duties and exercises its responsibilities in accordance with the provisions of the applicable legislation on cybersecurity, electronic signature, electronic identification, and trust services.

2. The Authority shall be responsible for organizing work for:

- a) the determination of cybersecurity measures and the supervision of their implementation by operators of critical and important information infrastructures;
- b) drafting and monitoring the implementation of the National Cybersecurity Strategy;
- c) the coordination of activities with other entities responsible for cybersecurity and cooperation at national and international levels with institutions and organizations in the field of cybersecurity;
- c) education and awareness raising in the field of cybersecurity;
- d) the implementation of security standards by certification service providers;
- dh) ensuring the quality, reliability, and compliance with legal standards for trust services and electronic identification;
- e) the control/monitoring of the implementation of standards and procedures for the issuance of qualified certificates by qualified trust service providers.

**III. ORGANIZATION AND FUNCTIONING OF THE NATIONAL CYBER SECURITY
AUTHORITY**

1. The Authority shall extend its activity throughout the entire territory of the Republic of Albania and is organized at the central level as a general directorate.

2. The Authority shall be headed by the director general, who organizes and supervises the activity of the institution and shall be responsible for its proper functioning, as well as represents the institution in relations with third parties.

3. The employment relations of the director general and the employees of the Authority shall be regulated on the basis of the provisions of Law no. 7961, dated 12.7.1995, “Labour Code of the Republic of Albania”, as amended.

4. The Director General shall be supported by 2 (two) Deputy General Directors. One of the directors of the content directorates of the Authority shall be appointed to the position of Deputy Director General, who, in addition to their functional duties, shall perform any other task assigned by the Director General to support him in the functioning of the institution.

5. The general director shall have the following duties and responsibilities:

a) ensure the implementation of legislation in the field of cybersecurity, electronic signature, as well as electronic identification and trust services;

b) sign cooperation agreements with domestic institutions and with foreign counterpart authorities or other entities abroad;

c) direct, processes the annual program for the commitments of the directorates and determines the priorities in their work;

ç) periodically report and whenever requested about the activity of the institution to the Prime Minister;

d) establish working groups for specific issues requiring the involvement of several departments of the Authority, as well as monitor the progress of fulfilling their purpose;

dh) take decisions on issuing administrative measures for administrative offences committed by entities under the applicable legislation on cybersecurity, electronic signatures, electronic identification, and trust services;

e) approve training programs for the professional training of the of the Authority's employees;

ë) prepare analyses, reports, and make proposals for the functioning of the structures under its authority;

f) ensure the proper management of the financial means and material resources of the institution;

g) perform any other function as the head of the institution, according to the current legislation on cybersecurity, electronic signature, electronic identification, and trust services.

6. The Authority, in fulfilment of its mission, areas of responsibility, and its functional responsibilities, shall perform the following tasks:

a) draft and monitor the implementation of the National Cybersecurity Strategy as the responsible institution, in coordination with other institutions responsible for cybersecurity;

b) identify critical and important information infrastructures, in cooperation and coordination with other entities responsible for cybersecurity;

c) act as the central contact point at the national and international level, as well as coordinate and harmonize the work with security and defence institutions, and cooperates with other entities responsible for cybersecurity, in accordance with the applicable legislation on cybersecurity;

ç) act in the capacity of the National CSIRT and CERT;

d) cooperate and exchange important information with operators of critical infrastructure and important information infrastructure, regarding the data in systems, when they are at risk due to a cyber incident;

(dh) determine and monitor the implementation of cybersecurity measures to be applied by operators of critical and important information infrastructures;

e) assists the operators of critical and important information infrastructures in the management of cyber incidents;

ë) actively monitor critical and important information infrastructures through information received from external platforms established by the NCSA or by the operators of information infrastructures, as well as from internal platforms, upon request from the operators of information infrastructures, for the purpose of identifying and preventing malicious actions;

f) cooperate with the responsible subjects of cybersecurity at national and international level;

g) prepare the national cybersecurity certification scheme, as well as encourage operators of information infrastructures to use it;

- gj) impose penalties on entities that do not fulfil legal obligations, according to the legislation in force on cybersecurity, electronic signature, electronic identification, and trust services;
- h) create and manage the register for documenting cybersecurity incidents;
- i) assess and analyse the security level of critical and important information infrastructure systems, through continuous controls and simulations, as well as determine additional measures for information infrastructure operators for the fastest and most efficient response to incidents or cyberattacks;
- j) register the conformity assessment bodies for cybersecurity for the assessment of cybersecurity measures;
- k) propose to the Prime Minister the declaration of a state of cyber crisis and the emergency measures for resolving the situation;
- l) periodically report on cyber incidents to ENISA and other international bodies, within the framework of the commitments of the Republic of Albania regarding Cybersecurity issues;
- ll) conduct awareness and educational activities in the field of cybersecurity for all groups of society;
- m) take the necessary measures, cooperate and coordinate work with the institutions responsible for the safety and protection of children and young people, for the creation of an environment *on-line* cyber safe in the Republic of Albania;
- n) identify, anticipate, and undertake the necessary measures for protection against potential cyber threats/attacks, in accordance with the applicable legislation on cybersecurity;
- nj) propose policies to guarantee Cybersecurity at national level, monitoring, identifying and responding to incidents for protection against cyberattacks/threats to critical and important information infrastructure in the Republic of Albania, as well as contribute to the drafting of policies for raising awareness of citizens, private entities, and public authorities about cyber risks;
- o) guarantee security for trust services, in particular for ensuring reliability and security in electronic transactions between citizens, private entities, and public authorities, by increasing the effectiveness of public and private services and electronic commerce;
- p) set the rules for secure electronic identification, electronic signature, electronic seals, qualified electronic timestamps, qualified electronic signature, qualified electronic seals, electronic transmission services, qualified electronic transmission services, website authentication, as well as guaranteeing a high level of security for electronic transactions in the Republic of Albania;
- q) establish the rules and methods for verifying the validity of products generated by trust services, domestic and foreign, enabling public access for checking their validity through the trust lists of the Member States of the European Union and the protocol *on-line* of the status of certificates and of certificate revocation lists;
- r) register and publishes on its official website the qualified providers of trust services;
- rr) temporarily, totally or partially suspend the activity of the certification service provider, when a violation of the legal provisions in force regarding electronic signature, electronic identification and trust services for exercising its activity is established;
- s) register and grant the status of “qualified” to the trust service provider, as well as supervise its activity;
- sh) supervise and monitor third parties, in cases where one or more of the obligations of trust services are transferred;
- t) carry out the control/monitoring of the implementation of standards and procedures for the issuance of qualified certificates by qualified trust service providers;
- th) supervise the process of issuing qualified electronic certificates and the implementation of electronic signature in public administration services;
- u) guarantee the implementation of standards for the secure identification of individuals to whom qualified electronic certificates are issued;

v) draft regulations and guidelines in accordance with international standards of the field, with the aim of ensuring secure electronic transactions and increasing the level of cybersecurity in important and critical information infrastructures in the Republic of Albania.

7. The Authority shall have its own emblem, logo, and official seal. The emblem of the Authority consists of the emblem of the Republic of Albania, with the inscriptions: “Republic of Albania, National Cyber Security Authority”, in accordance with the provisions of the decision of the Council of Ministers regarding the manner of use of the emblem of the Republic of Albania.

8. The seal of the Authority shall have the form and elements specified in the decision of the Council of Ministers regarding the rules for the production, administration, control, and preservation of official seals. The seal shall be produced, administered, and kept in accordance with the legislation in force.

9. The structure and the organisational structure of the Authority shall be approved by order of the Prime Minister, according to the provisions of the applicable legislation on the organization and functioning of the state administration.

10. The regulation on internal organization of work and conduct of the employees of the Authority shall be approved by the Prime Minister.

IV. FINAL PROVISIONS

1. Decision no. 141, dated 22.2.2017, of the Council of Ministers, “On the organization and functioning of the National Authority for Electronic Certification and Cybersecurity”, as amended, shall be repealed.

2. The National Cyber Security Authority shall be charged with the implementation of this decision. This Decision shall enter into force after its publication in the Official Journal.

DEPUTY PRIME MINISTER
Belinda Balluku