Pursuant to Article 95, item 3 of the Constitution of Montenegro, I hereby issue a

Decree on the Promulgation of the Law on Information Security

I promulgate the **Law on Information Security**, passed by the Parliament of Montenegro at the Third Session of the Second Regular (Autumn) Sitting in 2024, on November 19, 2024.

No: 011/24-1825/2-01

Podgorica, November 25, 2024

President of Montenegro,

Jakov Milatović, m.p.

LAW ON INFORMATION SECURITY*

The Law was published in the „Official Gazette of Montenegro," No. 113/2024 dated November 27, 2024, and entered into force on December 5, 2024

This Law is harmonized with Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

I. BASIC PROVISIONS

Subject
Article 1

This Law outlines the necessary information security measures for ensuring the utmost level of security for network and information systems, encompassing aspects such as cybersecurity, identification of essential and important entities, cybersecurity management, and other pertinent matters related to information security.

Obligation to apply
Article 2

The following are required to comply with this Law: state bodies, ministries, and other administration bodies, as well as local self-government units, local self-government bodies, and services established under the law governing local self-government, along with legal entities exercising public powers (hereinafter referred to as: bodies), companies and other legal entities, along with individuals who access or handle data and utilize and manage the network and information systems (hereinafter referred to as: other entities).

Information security
Article 3

Information security means the state of confidentiality, integrity, availability and protection of data, as well as cybersecurity.

Data confidentiality means the data is accessible solely to individuals authorized to gain access or handle such data.
Data integrity means maintaining the existence, accuracy, and completeness of data, along with the protection of processes or programs that inhibit unauthorized alterations to the data.
Data availability means that authorized users can access the data whenever they need it.

Essential and important entities
Article 4

Essential entities are bodies and other entities that utilize information and communication technologies to deliver services critical for the well-being, health, and safety of citizens, as well as the operation of the state, the functioning of which is vital for the execution of public interest activities, whose disruption or destruction could pose a threat to the life, health, and safety of citizens, and the operation of the state, irrespective of their size as defined by law governing accounting, particularly critical infrastructure operators in accordance with the law governing the designation and protection of critical infrastructure.
Important entities are bodies and other entities that utilize information and communication technologies and deliver services important for the well-being, health, and safety of citizens, as well as the operation of the state, the functioning of which is vital for the execution of public interest activities, whose disruption or destruction could impede the operation of the state, irrespective of their size in terms of the law governing accounting, particularly critical infrastructure operators in accordance with the law governing the designation and protection of critical infrastructure

CIRT of the state administration and a single national point of contact for information security
Article 5

The protection of network and information systems of state administration bodies against cyber threats, significant cyber threats and incidents is carried out by the state administration body responsible for the development of the information society and electronic administration (hereinafter referred to as the Ministry) through a special organizational unit (hereinafter referred to as CIRT of the state administration).
The Ministry represents the single national point of contact for information security and cooperates with the single national points of contact of other countries.

Cyber Security Agency
Article 6

The protection of network and information systems belonging to bodies and other entities, particularly those deemed essential and important, excluding state administration bodies, from cyber threats, significant cyber threats, and incidents, along with the professional oversight of the implementation of information security measures by these bodies and other entities, is conducted by the Cyber Security Agency (hereinafter referred to as the Agency).

Exemption from application
Article 7

This Law shall not apply to the state administration body responsible for defense affairs, the Army of Montenegro, the National Security Agency, the organizational unit of the state

administration body responsible for internal affairs that performs police work, Parliament of Montenegro and Central Bank of Montenegro, or the data whose information security is ensured in accordance with regulations which govern the confidentiality of data.

Personal data protection
Article 8

Personal data shall be used and processed in accordance with the law governing the personal data protection.

Use of gender-sensitive language
Article 9

The terms used in this Law for natural persons in the masculine gender imply the same terms in the feminine gender.

The meaning of the expressions
Article 10

The terms used in this Law shall have the following meanings:

1) **network and information system includes:**
   - an electronic communications network that includes transmission systems which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;
   - any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or
   - digital data stored, processed, retrieved or transmitted by elements covered under points (1) and (1) for the purposes of their operation, use, protection and maintenance;
2) **security of network and information systems** means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;
3) **data** means any information, message, or document that is generated, transmitted, received, stored, or displayed electronically, including through optical or similar means, and encompasses the transfer of such data over the Internet;
4) **encrypted data protection** is the application of software solutions or data protection devices that ensure the confidentiality, integrity and availability of data;
5) **cyber security** means the activity necessary to protect network and information systems against cyber threats and cyber incidents, as well as the users of such systems and other entities and persons affected by such cyber threats and incidents;
6) **cyber threat** means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact data or network and information systems, the users of such systems and other entities and persons;
7) **significant cyber threat** means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of these systems and other bodies or persons, by causing considerable material or non-material damage;

8) **incident** means an event compromising the confidentiality, integrity or availability of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;
9) **incident handling** means any actions and procedures aiming to detect, analyse, and contain or respond to an incident;
10) **vulnerability** means a weakness, susceptibility or flaw of a resource, system, process or control that can be exploited by a cyber threat;
11) **risk** means any circumstance or event having a potential adverse effect on the security of network and information systems;
12) **cyber crisis** is an event or situation in cyberspace that threatens the national security, health and life of a large number of citizens, significantly disrupts the environment or causes significant economic damage, and the response to such an event or situation requires the participation of several competent authorities, as well as the application of appropriate measure;
13) **cyberspace** means a conceptual space where Internet-based communication occurs.

II. INFORMATION SECURITY MEASURES

Types of information security measures
Article 11

Information security measures shall be:

1) data protection, and
2) protection against cyber threats and incidents.

Data protection
Article 12

Data protection means prevention and addressing harm resulting from the loss, unauthorized disclosure, or modification of data.
The protection outlined in the paragraph 1 of this Article shall encompass:

1) regulations for data management;
2) records of data access logs;
3) supervision of data security.

Protection against cyber threats and incidents
Article 13

Protection against cyber threats and incidents shall include:

1) physical protection;
2) network and information system protection;
3) risk management in the field of cyber security.

Physical protection
Article 14

Physical protection shall encompass the protection of the facility, the space, and the device housing the network and information systems.

Network and information systems protection
Article 15

The protection of the network and information systems shall encompass the protection of data that is processed, stored, or transmitted within network and information systems, along with the protection of the confidentiality, integrity, and availability of data throughout the stages of planning, designing, building, using, maintaining, and decommissioning the system.

Risk management in the field of cybersecurity
Article 16

Risk management in the field of cybersecurity includes:

1) conducting risk analysis and security analysis for the network and information systems;
2) establishing protocols for managing incidents (prevention, detection, and response to incidents);
3) adoption of a going concern plans and action in cyber crises;
4) adoption of an act governing the security of the supply chain involving the body, another entity responsible for managing the network and information systems, or the service provider;
5) adoption of an act governing the establishment, development, and maintenance of network and information systems, along with the information security of network and information systems;
6) implementation of encrypted data protection, provided that the nature of the work of the body, or another entity's requires it;
7) establishment of procedural guidelines for evaluating the efficacy of the measures outlined in points 1 to 6 of this Article.

Detailed content of information security measures
Article 17

Detailed content of information security measures referred to Articles 11 to 16 of this Law shall be prescribed by the Government of Montenegro (hereinafter: the Government).

Obligation to apply information security measures
Article 18

Bodies and other entities that are designated as essential and important entities in accordance with this Law shall be required to apply information security measures as outlined in Articles 11 to 16 of this Law.

Bodies and other entities that are not designated as essential and important entities in accordance with this Law shall be required to apply information security measures as outlined in Articles 11 to 15 of this Law.

Bodies and other entities shall appoint an employee to monitor the implementation of information security measures in accordance with paragraphs 1 and 2 of this Article.

To implement information security measures, bodies and other entities that are designated as essential entities in accordance with this Law must comply with the current Montenegrin standard for information security management MEST ISO/IEC 27001.

Accredited legal entity shall issue a certificate to essential entities concerning the adherence to the stipulations outlined in paragraph 4 of this Article.

The essential entities are required to request from the accredited entity regular confirmation of compliance with the stipulations outlined in paragraph 4 of this Article.

III. DESIGNATION OF ESSENTIAL AND IMPORTANT ENTITIES

Sectors and subsectors where essential and important entities are designated
Article 19

Essential entities shall be designated within the following sectors, or sub-sectors:

1) energy (electricity, district heating and cooling, oil, gas, hydrogen);
2) transport (air, rail, sea and road);
3) banking (credit institutions);
4) financial market infrastructure (trading venues and central counterparties defined by the law governing the capital market);

5) health (provision of health care at the primary, secondary and tertiary level, operations of national reference laboratories, registration and research of medicines);
6) drinking water (supply and distribution of water intended for human consumption);
7) waste water (collection, disposal or treatment of urban wastewater and industrial wastewater);
8) digital infrastructure (internet exchange point service providers, DNS service providers other than root name server operators, top-level domain name registry, cloud computing service providers, data center service providers, content delivery network providers, qualified trust service providers, providers of public electronic communications networks and of publicly available electronic communication services);
9) management of information and communication technologies services (information and communication technologies service providers);
10) public administration (public administration bodies and local self-government bodies);
11) space.

Important entities shall be designated within the following sectors, or sub-sectors:

1) postal and courier services (universal postal service providers, commercial postal service providers);
2) waste management (collection or transportation of waste, processing and disposal of waste);
3) manufacturing, production and distribution of chemicals (production and supply of chemicals in accordance with the law regulating chemicals);
4) production, processing and distribution of food (wholesale, industrial production and processing);
5) production (production of medical products and in vitro diagnostic medical products; production of computers, electronic and optical products; production of electrical equipment; production of machines and devices; production of motor vehicles, trailers and semi-trailers; production of other transport equipment);
6) providers of electronic services (online marketplace service providers);
7) research activity (entities with primary goal to conduct applied research or experimental development in order to use the results of that research for commercial purposes).

In addition to the entities referred to in paragraph 2 of this Article, important entities within the sector or sub-sector referred to in paragraph 1 of this Article, which are not defined as essential entities, may be designated as important entities, applying criteria referred to in Article 4 paragraph 2 of this Law.

Collection of data relevant to the determination of essential and important entities

Article 20

The relevant Ministry overseeing the specific sector or sub-sector where essential or important entities are designated (hereainafter referred to as the Competent Ministry) shall compile a comprehensive list of all bodies and other entities within that sector, or subsector and issue a request to these entities for the collection of pertinent data necessary for identifying essential and important entities.

Data important for designating essential and important entities shall be as follows:

1) the name of the body, or of other entity;
2) headquarters, that is, the address of the body, or of other entity;
3) tax identification number of the body or other entity;
4) name and surname of the responsible person in the body, or other entity;
5) single official address for electronic communication of the body or other entity;
6) contact telephone number of the responsible person in the body, or other entity;
7) data on the jurisdiction, that is, the activity of the body, or, of other entity;

8) data on which sector or sub-sector referred to in Article 19 paras. 1 and 2 of this Law the body, or other entity belongs to.

Bodies and other entities referred to in paragraph 1 of this Article shall submit the data referred to in paragraph 2 of this Article to the Competent Ministry within seven days from the day of receipt of the request.

Should there be a modification in the data specified in paragraph 2 of this Article, bodies and other entities are required to notify the Competent Ministry within 14 days from the date of the modification.

Proposal sectoral list of essential and important entities
Article 21

Based on the data referred to in Article 20 paragraph 2 of this Law, the Competent Ministry shall prepare a proposal sectoral list of essential and important entities.

The Competent Ministry shall submit the proposal sectoral list referred to in paragraph 1 of this Article to the Ministry.

List of essential and important entities
Article 22

Upon obtaining proposals for sectoral lists from the Competent Ministries, the Ministry shall compile a cohesive proposal for a list of essential and important entities and present it to the Government.

The Government, following the recommendation of the Ministry, shall establish the List of Essential and Important Entities.

The List provided in the paragraph 2 of this Article shall include the subsequent information regarding essential and important entities, specifically:

1) name;
2) headquarters, or address;
3) tax identification number.

The notification of essential and important entities
Article 23

Within seven days from the date of determination of the List of Essential and Important Entities, the Competent Ministry shall notify the designated essential and important entities in the respective sector or sub-sector of their designation as essential or important entities.

The Sectoral Register of Essential and Important Entities
Article 24

According to the List of Essential and Important Entities, the Competent Ministry shall keep the Sectoral Register of Essential and Important Entities. This Register shall include data referred to in Article 20 paragraph 2 points 1 to 7 of this Law, which shall pertain to essential and important entities within the sector or subsector for which the Ministry holds responsibility.

The Competent Ministry shall provide the information referred to in paragraph 1 of this Article to the Ministry to maintain the register referenced in Article 25 of this Law.

The Summary Register of Essential and Important Entities
Article 25

In accordance with the List of Essential and Important Entities and the data provided by the Competent Ministries as stipulated in Article 24 of this Law, the Ministry shall be responsible for maintaining the Summary Register of Essential and Important Entities.

The Summary Register of Essential and Important Entities shall include information from Article 20, paragraph 2, points 1 to 7, pertaining to all essential and important entities.

The Updating of registers and List of Essential and Important Entities
Article 26

Essential and important entities shall promptly notify the Competent Ministry regarding any changes to the information specified in Article 20, paragraph 2, points 1 to 7 of this Law, immediately following the occurrence of such changes.
According to the notification referred to in paragraph 1 of this Article, the Competent Ministry shall update the Sectoral Register of Essential and Important Entities and inform the Ministry regarding any changes in data.
In accordance with the notification outlined in paragraph 2 of this Article, the Ministry shall proceed to update the Summary Register of Essential and Important Entities.
Should it be established, based on the notification from paragraph 1 of this Article, that modifications or inclusions to the List of Essential and Important Entities are warranted, the Ministry shall draft a proposal for such modifications or inclusions to the List of Essential and Important Entities and present it to the Government for approval.

Confidentiality of data, registers and Lists of Essential and Important Entities
Article 27

Data referred to in Article 20 paragraph 2 of this Law and notification referred to in Article 20 paragraph 4 of this Law, the proposal of Sectoral List referred to in Article 21 of this Law, the proposal of the List and the List of Essential and Important Entities referred to in Article 22 of this Law, the notification referred to in Article 23 of this Law, the Sectoral Register referred to in Article 24 of this Law, the Summary Register referred to in Article 25 of this Law, the notifications referred to in Article 26 paragraphs 1 and 2 of this Law, as well as the proposed modifications to the List of Essential and Important Entities referred to in Article 26, paragraph 4 of this Law, shall be marked with the appropriate level of confidentiality, in accordance with the law governing data confidentiality.

IV. ASSESSMENT OF THE IMPACT OF CYBER THREATS, SIGNIFICANT CYBER THREATS AND INCIDENTS AND RESOLUTION OF INCIDENTS AND CYBER CRISIS

Criteria for assessing the impact of cyber threats, significant cyber threats and incidents
Article 28

In the event of the occurrence of a cyber threat, a significant cyber threat, or an incident affecting the network and information systems, it is imperative for bodies and other entities to assess the impact of such cyber threats or incidents on the ongoing provision of services.
The assessment presented in paragraph 1 of this Article shall rely on the subsequent criteria:

1) the count of users unable to utilize the service;
2) the count of users who experienced considerable challenges in utilizing the service;
3) the length of the cyber threat, serious cyber threat, or incident;
4) the spatial allocation of the cyber threat, significant cyber threat, or incident (if it can be ascertained).

Cyber threat, significant cyber threat and incident not impacting the ongoing provision of services
Article 29

Should it be determined, according to the criteria outlined in Article 28 paragraph 2 of this Law, that a cyber threat, a significant cyber threat, or an incident do not impact the ongoing provision of services, a monthly report regarding these cyber threats and incidents shall be submitted by bodies and other entities, excluding state administration bodies, to the Agency, while state administration bodies shall report to the CIRT of the State Administration.
In the case referred to in paragraph 1 of this Article, the bodies and other entities shall address cyber threats, significant cyber threats, or incidents independently, without the involvement of the Agency or the CIRT of the State Administration.

Cyber threat, significant cyber threat and incident that adversely affect the ongoing provision of services
Article 30

In the event that, based on the criteria referred to in Article 31 paragraph 2 of this Law, it is estimated that a cyber threat, a significant cyber threat, or an incident could have a significant adverse impact on the ongoing provision of services, the bodies and other entities, except for the state administration bodies, shall submit initial notification on these cyber threats and incidents to the Agency, while the state administration bodies shall notify the CIRT of the State Administration.
The initial notification shall be submitted within 24 hours of becoming aware of the cyber threat, signficant cyber threat or the incident, using the designated form.
The Ministry shall prescribe the format and content of the initial notification form.

Determining the level of adverse impact of cyber threats, significant cyber threats and incidents on the ongoing provision of services
Article 31

Upon receiving the initial notification, the Agency, or CIRT of the State Administration, shall undertake an analysis of the impact of a cyber threat, a significant cyber threat, or an incident on the ongoing provision of services and potential responses to such cyber threats or incidents and categorize the severity of the incident as low, medium, or high.
The method for conducting the analysis and the criteria for assessing the level of the incident outlined in paragraph 1 of this Article shall be established by the Government.

Low-level incident
Article 32

Upon receiving the initial notification, if it is assessed that the incident is of a low level, the Agency, or the CIRT of the State Administration, shall, within 24 hours, provide the body or other entity with guidelines for responding to the incident, if deemed necessary.

Medium-level incident
Article 33

Upon receiving the initial notification, if it is assessed that the incident falls within a medium level, the Agency, or the CIRT of the State Administration, shall promptly, and no later than 24 hours after receiving the notification, issue guidelines for addressing the incident and engage in its resolution.
Throughout the timeframe of the incident mentioned in paragraph 1 of this Article, it shall be mandatory for bodies and other entities to provide, within 72 hours of the initial notification,

an initial report to the Agency, or CIRT of the State Administration on the duration of the incident and the measures taken to address it, on the designated form.
Should, for the duration of the incident referred to in paragraph 1 of this Article, bodies and other entities become aware of new data or circumstances that may have an impact on such incident, they shall submit a special report to the Agency, or CIRT of the State Administration, without delay on a designated form.
Should the incident referred to in paragraph 1 of this Article persist beyond the deadline outlined in paragraph 2 of this Article, it shall be mandatory for bodies and other entities to provide ongoing reports to the Agency, or CIRT of the State Administration, every 72 hours, on the duration of the incident and measures taken to resolve it, using the designated form.
Following the resolution of the incident mentioned in paragraph 1 of this Article, and no later than 30 days after the resolution thereof, the bodies and other entities shall submit a final report regarding the incident to the Agency, or the CIRT of the State Administration, using the designated form.
The format and substance of the report forms outlined in paragraphs 2 to 5 of this Article shall be mandated by the Ministry.

High-level incident
Article 34

If, upon receiving the initial notification, it shall be determined that the incident is of a high level, the Agency shall notify the CIRT of the State Administration, or the CIRT of the State Administration shall notify the Agency, without delay, in writing.
In the case referred to in paragraph 1 of this Article, the Agency and the CIRT of the State Administration shall collaboratively engage in addressing the incident and offer the body and other entities guidelines for managing the situation.
Throughout the timeframe of the incident referred to in paragraph 1 of this Article, it shall be mandatory for bodies and other entities to provide the initial report detailing the duration of the incident and the measures undertaken to address it to the Agency, or CIRT of the State Administration, within 72 hours following the submission of the initial notification, using the designated form.
In the event that, during the incident mentioned in paragraph 1 of this Article, the bodies and other entities acquire new information or circumstances that could influence the incident, they shall promptly submit a special report to the Agency, or CIRT of the State Administration, using the designated form.
Should the incident mentioned in paragraph 1 persist beyond the deadline outlined in the paragraph 3, it shall be mandatory for the bodies and other entities to provide ongoing reports to the Agency, or CIRT of the State Administration, every 24 hours, regarding the duration of the incident and the measures undertaken to address it, using the designated form.
Following the resolution of the incident referred to in paragraph 1 of this Article, and within a maximum of 30 days from the date of resolution, the bodies and other entities shall submit the final report regarding such incident to the Agency, or CIRT of the State Administration, using the designated form.
The format and substance of the report forms outlined in paragraphs 3 to 6 of this Article shall be mandated by the Ministry.

Cyber crisis
Article 35

Where the Agency and the CIRT of the State Administration are unable to resolve a high-level incident within ten days from the date of the initial notification in line with Artcile 34 of this Law, the Ministry, having previously obtained the opinion of the Agency, shall submit a proposal to the Government for the declaration of a cyber crisis.

The proposal outlined in paragraph 1 of this Article shall detail the incident, the actions implemented, the rationale behind the declaration of a cyber crisis, and the proposed measures to address such crisis.
Following the proposal outlined in paragraph 1 of this Article, the Government shall render a decision regarding the declaration of a cyber crisis, implement measures to address the cyber crisis and designate the bodies required to engage in the resolution of the crisis.
The Ministry shall oversee the operations of the entities referred to in paragraph 3 of this Article in addressing the cyber crisis and provide weekly reports to the Government on all activities undertaken.
The Agency, in collaboration with the Ministry, shall oversee the operational coordination for addressing the cyber crisis in alignment with the National Plan for Responding to Cyber Threats, Significant Cyber Threats, Incidents, and Cyber Crises.
Following the resolution of the cyber crisis, the Ministry, in collaboration with the Agency, shall compile a final report regarding the cyber crisis and formulate a proposal to officially declare the cessation of the cyber crisis, which is then presented to the Government.
In accordance with the reports and proposals outlined in paragraph 6 of this Article, the Government shall reach a decision on the conclusion of the cyber crisis.

Assistance in resolving incidents and cyber crises
Article 36

The Agency and CIRT of the State Administration may seek assistance from both domestic and international institutions and organizations to address medium-level or high-level incidents and cyber crises, as well as to share information with those institutions and organizations.

Confidentiality of notifications, reports and guidelines
Article 37

The reports referred to in Article 29 paragraph 1 of this Law, the initial notifications referred to in Article 30 paragraph 1 of this Law, the guidelines referred to in Article 32 and Article 33 paragraph 1 of this Law, the reports referred to in Article 33 paragraphs 2 to 5 of this Law, the notifications referred to in Article 34 paragraph 1 of this Law, the guidelines referred to in Article 34 paragraph 2 of this Law, the reports referred to in Article 34 paragraphs 3 to 6 of this Law, the proposals and opinions referred to in Article 35 paragraph 1 of this Law, the decisions referred to in Article 35 paragraph 3 of this Law, the reports referred to in Article 35 paragraph 4 of this Law, as well as the reports and proposals referred to in Article 35 paragraph 6 of this Law shall be assigned an appropriate level of confidentiality in compliance with the law governing data confidentiality.

V. THE MINISTRY AND CIRT OF THE STATE ADMINISTRATION

Competencies of the Ministry
Article 38

The Ministry shall:

1) propose to the Government strategies and action plans, along with regulations concerning information security;
2) formulate the National Plan for Responding to Cyber Threats, Significant Cyber Threats, Incidents, and Cyber Crises, in collaboration with the Agency;
3) conduct screening of the network and information systems of state administration bodies, with the aim of identifying any weaknesses within those systems;

4) issue directives and protocols that are implemented when evaluating the information security of network and information systems within state administration bodies;
5) issue alerts, notifications, and information regarding risks and incidents to state administration bodies;
6) address reported incidents concerning network and information systems of state administration bodies;
7) maintain documentation of reported incidents within the network and information systems of state administration bodies;
8) collaborate with the Agency to facilitate the exchange of information regarding cyber threats, significant cyber threats, incidents, and the resolution of those threats, incidents, and cyber crises, in accordance with this Law;
9) to enhance information security, collaborate with national and international institutions and organizations, along with the private and civil sectors;
10) present to the Government a report regarding the status of information security for network and information systems utilized by state administration bodies at least annually;
11) provide additional reports to the Government, as stipulated by this Law;
12) carry out other responsibilities as outlined by this Law.

CIRT of the State Administration
Article 39

Responsibilities outlined in Article 38 paragraph 1 points 3 to 9 of this Law shall be executed by the CIRT of the State Administration.
The CIRT of the State Administration shall adhere to specific technical and other conditions, which include the following:

1) maintaining uninterrupted communication capabilities, ensuring multiple two-way communication options are available at all times;
2) securing workspaces and information systems in protected locations;
3) implementing a robust incident reporting and management system;
4) safeguarding the confidentiality and integrity of operational processes;
5) establishing redundant systems and backup workspaces to guarantee operational continuity;
6) employing an adequate workforce to support continuous operations around the clock.

Redundant systems, as outlined in paragraph 2 point 5 of this Article, shall serve as backup systems that take over when the primary system’s operation has been disrupted.

VI. CYBER SECURITY AGENCY

Agency jobs
Article 40

The Agency shall:

1) monitor and evaluate the implementation of regulations, strategies, and action plans related to information security, provide suggestions and recommendations for enhancing information security measures;
2) monitor and evaluate the regulations set forth by the European Union and NATO member countries regarding information security;

3) conduct proactive assessments of networks and information systems belonging to essential and important entities that are not state administration bodies, while ensuring their prior consent is obtained;
4) issue directives and protocols that are implemented during the evaluation of information security for network and information systems of bodies and other entities, excluding state administration bodies;
5) issue warnings, notifications, and information regarding risks and incidents to bodies and other entities, excluding state administration bodies;
6) address reported incidents on the network and information systems of bodies and other entities, excluding state administration bodies;
7) maintain documentation of reported incidents within the network and information systems of bodies and other entities, excluding state administration bodies;
8) conduct specialized oversight regarding the execution of information security measures by bodies and other entities, excluding state administration bodies;
9) conduct expert oversight by assessing whether essential entities possess a certificate confirming compliance with the valid Montenegrin standard for information security management MEST ISO/IEC 27001 and whether they have sought regular verification of compliance with that standard;
10) engage in the execution of international projects related to information security;
11) conduct training for personnel in bodies and other entities to enhance information security;
12) collaborate with the Ministry to facilitate the exchange of information regarding cyber threats, significant cyber threats, incidents, and the resolution of such threats, incidents, and cyber crises, in accordance with this Law;
13) to enhance information security, collaborate with both national and international institutions and organizations, along with the private and civil sectors;
14) present to the Government a report regarding the status of information security for network and information systems of bodies and other entities, particularly essential and important entities, which do not fall under the category of state administration bodies, at least annually.

Bodies of the Agency
Article 41

The bodies of the Agency shall be: the Council of the Agency and the Director of the Agency.

The Council of the Agency
Article 42

The Council of the Agency shall have a president and four members who shall be appointed and dismissed by the Government.
The President of the Council of the Agency shall be proposed by the Ministry, and one member of the Council of the Agency shall be proposed by:
1) the University of Montenegro;
2) the Chamber of Commerce of Montenegro;
3) the General Secretariat of the Government of Montenegro;
4) the Agency, from among its employees.

The President and members of the Council of the Agency shall be appointed for a period of four years.

The jobs of the Council of the Agency
Article 43

The Agency Council shall:
1) enact the Articles of Association of the Agency;
2) establish the annual work program and financial plan of the Agency;
3) prepare and present to the Government the annual work report and financial report of the Agency;

4) appoint and dismiss the director of the Agency;
5) determine the training plan for the professional development of the employees of the Agency;
6) adopt the Code of Ethics for employees of the Agency;
7) perform other duties in accordance with applicable regulations and the Agency's Articles of Association.

The financial plan of the Agency shall be implemented solely after obtaining the requisite approval from the relevant state administration body overseeing financial matters.

Termination of the term of office of the president and member of the Council of the Agency
Article 44

The term of office of the President or a member of the Council of the Agency shall terminate:
1) at the end of the period for which appointed;
2) by resignation;
3) by dismissal.

The President, that is, a member of the Council of the Agency, shall be dismissed in cases where he/she:
1) is sentenced to unconditional imprisonment;
2) has been found guilty of an offense that renders him/her unfit for fulfilling his/her responsibilities;
3) engages in actions that violate the law or acts of the Agency;
4) unprofessionally or negligently performs the tasks for which appointed.

Director of the Agency
Article 45

The appointment of the Director of the Agency shall be conducted through a public competition that is announced by the Council of the Agency.
An individual who, alongside the general qualifications for positions within state bodies, fulfills the subsequent criteria, may be appointed as the Director of the Agency:
1) Qualification level of education at VII1, and
2) Relevant work experience, as outlined below:
   - five years of professional experience in the domain of information security, or
   - seven years of professional experience in government bodies or state administration bodies, or ten years of professional experience, including five years in management roles.

The term of the Director of the Agency shall be set for a duration of five years.

The reponsibilities of the Director of the Agency
Article 46

The Director of the Agency shall:
1) monitor and direct the Agency;
2) act on behalf of the Agency and ensure the compliance and standards of quality in the Agency's operations;
3) arrange tasks within the Agency;
4) submit to the Agency Council the Agency's Articles of Association, the annual work program and financial plan, the annual work report and financial report of the Agency, along with other decisions;

5) implement the decisions of the Agency's Council;
6) monitor personnel and financial resources;
7) establish the act on the internal organization and systematization of the Agency;
8) ensure the visibility of the Agency's activities;
9) suggest a training program for the professional development of the Agency's staff;
10) collaborate with national and international organizations, along with the private and civil sectors, to enhance information security;
11) carry out additional duties in alignment with the law and the Agency's Articles of Association.

The act on internal organization and systematization of the Agency shall be enacted with the prior approval of the relevant state administration body overseeing financial matters.

Termination of the mandate of the Director of the Agency
Article 47

The law governing the rights and responsibilities of civil servants and state employees, which pertain to the cessation of the mandate of the head of the state administration body, shall be applicable to the cessation of the mandate of the Agency's Director.

Status of the Agency
Article 48

The Agency shall have the status of a legal entity as well as that of a state agency.
The Agency shall bear responsibility to the Government for its actions.
The Government shall be responsible for making the decision regarding the establishment of the Agency.

Statute of the Agency
Article 49

The Agency shall have the Articles of Association.
The Agency's Articles of Association shall govern the location of the Agency's headquarters, outline the internal organization, define the operational procedures, decision-making processes, and the responsibilities of the Agency's bodies, as well as the transparency of its activities and other significant matters pertaining to the Agency's operations.
The Government shall grant approval for the Articles of Association of the Agency.

Funding of the Agency
Article 50

The budget of Montenegro shall allocate funds for the operation of the Agency.
The Agency shall organize and manage its financial operations in accordance with the regulations governing the area of the budget system and financial reporting.

Application of other regulations
Article 51

The regulations governing civil servants and state employees shall be applicable to the rights, duties, and responsibilities of the Agency's employees.
Employees engaged in information security roles within the Agency shall form an employment relationship without the necessity of a public announcement process, and such positions must be acknowledged through an act pertaining to internal organization and systematization.

VII. PROFESSIONAL SUPERVISION

Supervisor
Article 52

The Agency shall conduct professional oversight through its employees, who are empowered to carry out such supervision in line with the act on internal organization and systematization of the Agency (hereinafter referred to as the supervisor).
A supervisor may be a person who, alongside the general criteria for forming an employment relationship in state bodies, shall fulfill the subsequent requirements, specifically possessing:

1) an VII1 qualification level of education, and
2) five years of professional experience in the domain of information security.

Supervisor's authorities
Article 53

During professional supervision, the supervisor shall possess the power to control the implementation of information security measures referred to in Articles 11 to 15 of this Law with bodies and other entities, excluding state administration bodies.
Alongside the powers outlined in paragraph 1 of this Article, during the professional supervision process, the supervisor shall be empowered to oversee the implementation of information security measures specified in Article 16 of this Law at essential and important entities, with the exception of state administration bodies.
Alongside the powers outlined in paragraphs 1 and 2 of this Article, during the course of professional supervision, the supervisor shall be empowered to verify with essential entities, excluding state administration bodies, whether these entities possess a certificate confirming their compliance with the valid Montenegrin standard for information security management MEST ISO/IEC 27001 and whether they have sought regular assessments of their compliance with that standard.

Obligations of essential and important entities when performing professional supervision
Article 54

To conduct professional supervision, bodies and other entities, excluding state administration bodies, shall grant the supervisor access to the premises, computer equipment, and devices. They shall also be required to promptly provide or submit for review any necessary data and documentation pertinent to the supervision subject.

Minutes
Article 55

The supervisor shall compile minutes regarding the conducted professional supervision and present it to the body, or the other entity where the supervision took place, within three days following the completion of the supervision.

Elimination of irregularities
Article 56

Should any irregularities be identified during the professional supervision, the supervisor shall notify the relevant body, or other entity where the irregularities have been detected, and

provide a suitable timeframe for rectifying these irregularities, which shall be documented in the minutes as outlined in Article 55.
Should the body or other entity fail to rectify the irregularities as stipulated in paragraph 1 of this Article, the supervisor shall present the minutes referenced in Article 55 of this Law to the Director of the Agency.
In case referred to in paragraph 2 of this Article, the Director of the Agency shall issue a decision mandating actions to rectify the irregularities.
An administrative proceedings may be brought against the decision outlined in paragraph 3 of this Article.

Application of other regulations in the exercise of professional supervision
Article 57

The regulations governing inspection supervision and administrative proceedings shall be applied accordingly to the procedures and methods of conducting professional supervision, the responsibilities and authorities of supervisors, and other significant matters related to the execution of professional supervision, unless stated otherwise by this Law.

Handling of data
Article 58

The supervisor shall maintain and safeguard the information acquired during the execution of professional supervision, in line with the laws governing data confidentiality, personal data protection, and the safeguarding of business secrets.

Official identification card of the supervisor
Article 59

An official identification card shall be granted to the supervisor to validate his position as a supervisor.
The official identification card referred to in paragraph 1 of this Article shall be provided by the Agency using the designated form.
Should there be a loss or disappearance of the official identification card mentioned in paragraph 1 of this Article, the supervisor shall notify the Director of the Agency within three days of the loss or disappearance of the official identification card and declare the identification card invalid in the “Official Gazette of Montenegro”.
Upon the conclusion of the employment relationship within the Agency, or at the cessation of the supervisor’s status, the supervisor shall return the official identification card referred to in paragraph 1 of this Article to the Agency.
The Agency shall maintain documentation regarding the issuance and return of official identification cards as outlined in paragraph 1 of this Article. This documentation shall include: serial number, first and last name of the supervisor, serial number of the identification card, date of issue, date of return, or instances of loss or disappearance of the identification card, signature of the supervisor, and an accompanying note.
The Agency shall establish the form and substance of the official identification card form referred to in paragraph 1 of this Article.

Technical and other conditions
Article 60

The Agency shall comply with the technical and additional requirements outlined in Article 39, paragraph 2 of this Law.

VIII. INFORMATION SECURITY COUNCIL

The establishment of the Information Security Council
Article 61

To monitor the advancement of information security, particularly in the realm of cybersecurity, and to guarantee a secure cyberspace in Montenegro, the Government shall form the Information Security Council.
The Information Security Council shall be established for a term of four years.

The composition of the Information Security Council
Article 62

The Information Security Council shall be composed of representatives from the Ministry, the Agency, the state administration body in charge of internal affairs, the state administration body overseeing defense matters, the state administration body responsible for judicial matters, the state administration body responsible for foreign affairs, the state administration body responsible for confidential data, and the National Security Agency. Additionally, representatives from other authorities and institutions may be included as needed.
The Ministry shall carry out professional and administration-technical tasks to support the Information Security Council's requirements.

Act on the establishment of the Information Security Council
Article 63

The act regarding the formation of the Information Security Council shall outline its responsibilities, operational procedures, and other significant matters pertaining to its functions.

IX. INSPECTION SUPERVISION

Administrative supervision
Article 64

The Ministry shall be responsible for overseeing the execution of this Law, along with other regulations and acts adopted on the basis of this Law.

Inspection supervision
Article 65

Inspection supervision of the execution of information security measures by state administration bodies shall be conducted by the inspector for information society services (hereinafter: inspector) in accordance with this Law and the law governing inspection supervision.

Special powers of the inspector
Article 66

During the course of inspection supervision, the inspector, alongside the powers defined by the law governing inspection supervision, shall possess the authority to oversee the enforcement of information security measures within state administration bodies as outlined in Articles 11 to 15 of this Law.
Alongside the powers referred to in paragraph 1 of this Article, during the inspection supervision process, the inspector shall be empowered to oversee the implementation of

information security measures outlined in Article 16 of this Law at state administration bodies identified as essential and important entities in accordance with this Law.
Alongside the powers outlined in paragraphs 1 and 2 of this Article, during the course of inspection supervision, the inspector shall be empowered to verify with designated state administration bodies that are recognized as esential entities in accordance with this Law, whether these bodies hold a certificate confirming compliance with the current Montenegrin standard for information security management MEST ISO/IEC 27001, and whether they have required the periodic assessments to ensure adherence to that standard.

The obligations of state administration bodies when performing inspection supervision
Article 67

To conduct inspection supervision, state administration bodies must grant the inspector access to the premises, computer systems, and devices, as well as promptly provide or deliver the necessary data and documentation pertinent to the subject of supervision.

X. PENAL PROVISIONS

Article 68

A legal entity – an essential entity - shall incur a fine for a misdemeanor ranging from 500 to 20,000 euros, if:

1) failing to apply information security measures referred to in Articles 11 to 16 of this Law (Article 18 paragraph 1);
2) failing to meet the requirements in accordance with the current Montenegrin standard for information security management MEST ISO/IEC 27001 (Article 18 paragraph 4);
3) failing to require the accredited legal entity to periodically check the fulfillment of the conditions in accordance with the current Montenegrin standard for information security management MEST ISO/IEC 27001 (Article 18 paragraph 6);
4) failing to submit to the Competent Ministry a notification on the change of data referred to in Article 20, paragraph 2, points 1 to 7 of this Law, immediately after the occurrence of the change (Article 26 paragraph 1).

For the misdemeanor referred to in paragraph 1 of this Article, the responsible person in the legal entity shall be fined in the amount ranging from 30 euros to 1,500 euros.

Article 69

A legal person - an important entity - shall incur a fine for a misdemeanor ranging from 500 to 20,000 euros, if:

1) failing to apply information security measures referred to in Articles 11 to 16 of this Law (Article 18 paragraph 1);
2) failing to submit to the Competent Ministry a notification about the change of data referred to in Article 20 paragraph 2 points 1 to 7 of this Law, immediately after the occurrence of the change (Article 26 paragraph 1).

For the misdemeanor referred to in paragraph 1 of this Article, the responsible person in the legal entity shall be fined in the amount ranging from 30 euros to 1,500 euros.

Article 70

A legal entity shall be fined in the amount ranging from 500 to 5,000 euros for a misdemeanor, if:

1) failing to apply information security measures referred to in Articles 11 to 15 of this Law (Article 18 paragraph 2);
2) failing to appoint an employee to monitor the implementation of information security measures (Article 18 paragraph 3);
3) failing to submit data to the Competent Ministry within seven days from the date of receipt of the request (Article 20 paragraph 3);
4) failing to notify the Competent Ministry about the change of data within 14 days from the date of occurrence of the change (Article 20 paragraph 4);
5) failing to submit a report on cyber threats, serious cyber threats, or incidents once a month to the Agency, or CIRT of the State Administration (Article 29 paragraph 1);
6) failing to submit an initial notification to the Agency, or CIRT of the State Administration, about a cyber threat, a serious cyber threat, or an incident that could significantly affect the ongoing service provision (Article 30 paragraph 1);
7) failing to submit the initial notification on the cyber threats, serious cyber threats or incidents, on the prescribed form within 24 hours of learning about the incident (Article 30 paragraph 2);
8) within 72 hours from the submission of the initial notification, the Agency or CIRT of the State Administration failing to submit the initial report on the duration of the medium-level incident and the measures taken to resolve such incident, on the prescribed form (Article 33 paragraph 2);
9) failing to submit a special report on the prescribed form to the Agency, i.e. CIRT of the State Administration without delay, while learning, during the medium-level incident, of new data or circumstances that may have an impact on such incident (Article 33 paragraph 3);
10) failing to submit ongoing reports on the duration of the incident and the measures taken to resolve the medium-level incident, on the prescribed form, to the Agency, that is, to the CIRT of the State Administration, every 72 hours (Article 33 paragraph 4);
11) failing to submit a final report on a medium-level incident to the Agency, that is, to the CIRT of the State Administration, no later than 30 days after the resolution of such incident, on the prescribed form (Article 33 paragraph 5);
12) within 72 hours from the submission of the initial notification, failing to submit the initial report on the duration of the high-level incident and the measures taken to resolve the incident, on the prescribed form, to the Agency or CIRT of the State Administration (Article 34 paragraph 3);
13) failing to submit a special report on the prescribed form to the Agency, or CIRT of the State Administration without delay, while, during the high-level incident, learning of new data or circumstances that may have an impact on such incident (Article 34 paragraph 4);
14) failing to submit ongoing reports on the duration of the incident and the measures taken to resolve the incident, on the prescribed form, every 24 hours, to the Agency, or CIRT of the State Administration (Article 34 paragraph 5);
15) failing to submit a final report on a medium-level incident to the Agency, or CIRT of the State Administration, no later than 30 days from the day the incident was resolved, on the prescribed form (Article 34 paragraph 6).

For the misdemeanor referred to in paragraph 1 of this Article, the responsible person in the legal entity shall be fined in the amount ranging from 30 euros to 1,500 euros.

In the case of repeated violations referred to in paragraph 1 of this Article, a ban on the performance of a calling, activity or duty shall be imposed for a period of three to six months.

XI. TRANSITIONAL AND FINAL PROVISIONS

Deadline for adoption of by-laws
Article 71

By-laws for the implementation of this Law shall be adopted within six months from the date of entry into force of this Law.
Until the adoption of by-laws referred to in paragraph 1 of this Article, the by-laws adopted on the basis of the Law on Information Security ("Official Gazette of Montenegro", No. 14/10, 40/16 and 67/21) shall apply.

The deadline for submitting proposals for sectoral lists
Article 72

Competent Ministries shall submit proposals for sectoral lists referred to in Article 21 paragraph 1 of this Law to the Ministry, no later than nine months from the date of entry into force of this Law.

Deadline for obtaining the certificate
Article 73

Essential entities shall obtain a certificate of fulfillment of the conditions in accordance with the current Montenegrin standard for information security management MEST ISO/IEC 27001, within 30 months from the date of entry into force of this Law.

Deadline for establishment of the Agency
Article 74

The decision on the establishment of the Agency shall be made within 15 days from the date of entry into force of this Law.

Deadline for appointing the President and members of the Council of the Agency
Article 75

The appointment of the President and members of the Council of the Agency shall be made within 60 days from the date of entry into force of this Law.

Deadline for appointing the Director of the Agency
Article 76

The appointment of the Director of the Agency shall be carried out within 90 days from the day of the election of the Council of the Agency.
Until the appointment of the Director of the Agency, in accordance with this Law, the duties of the Director of the Agency shall be performed by an acting official, who, on the proposal of the Minister of Public Administration, shall be appointed by the Government.
The proposal referred to in paragraph 2 of this Article shall be submitted to the Government within 15 days from the date of entry into force of this Law.

Adoption of acts of the Agency
Article 77

The Articles of Association of the Agency, the act on the internal organization and systematization of the Agency, the Rules of Procedure of the Council and other acts of the Agency shall be adopted within 90 days from the day of the election of the Acting Director of the Agency.

Transfer of civil servants
Article 78

Upon the adoption of the act on the internal organization and systematization of the Agency, the Agency shall assume from the Directorate for the Protection of Confidential Data civil servants engaged in duties within the CIRT organizational unit, along with the associated equipment and official documentation.
Civil servants referred to in paragraph 1 of this Article shall maintain the positions they held before being transferred, until the adoption of the act on deployment, in line with the act on the internal organization and systematization of the Agency.
Civil servants referred to in paragraph 1 of this Article who are not deployed in accordance with the act on the internal organization and systematization of the Agency shall exercise their rights as stipulated by the regulations governing civil servants and state employees.

Continuance of the Information Security Council operation
Article 79

The Information Security Council, which is established in accordance with the Law on Information Security ("Official Gazette of Montenegro", No. 14/10, 40/16 and 67/21), shall continue its work until the Information Security Council is established in accordance with this Law.

Termination of validity of regulations
Article 80

On the date of entry into force of this Law, the Law on Information Security ("Official Gazette of Montenegro", No. 14/10, 40/16 and 67/21) and the provisions of Article 74 paragraph 1 item 8b and Article 74a of the Law on Data Confidentiality ("Official Gazette of Montenegro", No. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13, 18/14, 48/15 and 74/20) shall cease to be valid.

Entry into force
Article 81

This Law shall enter into force on the eighth day following the day of its publication in the "Official Gazette of Montenegro".

Number: 10-2/24-1/19
EPA 246 XXVIII
Podgorica, November 19, 2024

The Parliament of Montenegro of the 28th convocation

President,
Andrija Mandić, s.r.