LAW No 58, dated March 14th, 2023
on Romania's cyber security and defense, and for amending and completing some normative acts

ISSUER: The Parliament
PUBLISHED IN: Official Gazette No 214, dated March 15th, 2023

Effective date: March 18th, 2023

Consolidated form valid on March 13th, 2024

The hereby consolidated form shall be valid from March 18th, 2023 to March 13th, 2024

The Parliament of Romania passes the present law.

CHAPTER. I
General provisions

ARTICLE 1
(1) This Law sets out the legal and institutional framework regarding the organization and conduct of activities in the field of cyber security and defense, cooperation mechanisms and responsibilities of the institutions with tasks in the fields stipulated above.
(2) Cyber security and defense are achieved through the adoption and implementation of policies and measures for the purpose of knowing, preventing and countering vulnerabilities, risks and threats within the cyberspace.

ARTICLE 2
For the purposes of this Law, the terms and expressions written bellow have the following meaning:
a) cyber defense - the totality of activities, means and measures used to counter cyber threats and mitigate their effects on communication systems and information technology, weapon systems, networks and information systems, which support military defense capabilities;
b) cyber threat - as defined in art. 2 let. f) of Government Emergency Ordinance no. 104/2021 on the establishment of the National Cybersecurity Directorate, passed with amendments and additions by Law no. 11/2022, with subsequent amendments;
c) cyber-attack - hostile action in cyberspace that can affect cybersecurity;
d) cybersecurity audit - an activity that makes a systematic assessment of all policies, procedures and protection measures implemented at the level of certain IT networks and systems, in order to identify malfunctions and vulnerabilities and provide remedial solutions;
e) Advanced Persistent Threat, hereinafter referred to as APT - as defined in Article 2 paragraph a) of The Government Emergency Ordinance 89/2022 on the establishment, administration and development of cloud-based IT infrastructure and services used by public authorities and institutions;
f) Operational Security Center - team of experts in cybersecurity, which has the role of monitoring, analyzing and responding to cybersecurity incidents;

g) cyber crisis - as defined in Article 2 paragraph k) of Government Emergency Ordinance no. 104/2021, passed with amendments and additions by Law no. 11/2022, as amended;
h) cyber intelligence - activities of collecting, processing, analytical processing and valorization of data and information on actions that affect national security interests and objectives on the information and communication technology line, as well as the identification, knowledge, prevention and counteraction of any actions in cyberspace that may pose risks, vulnerabilities and/or threats to the national security and defense of Romania;
i) cyber counter-intelligence - all offensive and defensive activities, means and measures to identify, deter, neutralize and protect against information activities on hostile actions that affect national security interests and objectives, carried out in cyberspace and in the field of defense;
j) cyber diplomacy - the diplomatic activity through which the promotion of the foreign and security policy interests of Romania is achieved within the bilateral and multilateral formats of dialog and negotiation on topics relevant to the field of cyber security at national and international level. The activity includes the promotion of objectives deriving both from the need to ensure and strengthen national cybersecurity and from Romania's foreign policy priorities;
k) cybersecurity incident response team - as defined in art. 2 paragraph a) of Government Emergency Ordinance no. 104/2021, passed with amendments and additions by Law no. 11/2022, as amended;
l) provider of cybersecurity technical services - natural and/or legal person who performs, in order to protect network and information systems, at least one of the following activities: implementation of cybersecurity measures, evaluation, monitoring and testing of implemented measures, as well as management of cybersecurity risks, threats, vulnerabilities and incidents;
m) cyber hygiene - routine measures regularly applied by natural and legal persons, which are designed to reduce their exposure to the risks posed by cyber threats, in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on cybersecurity certification for information and communication technology and repealing Regulation (EU) No 526/2013, hereinafter referred to as the Cybersecurity Regulation;
n) cybersecurity incident - an event in cyberspace that disrupts the functioning of one or more computer networks and systems and whose consequences are liable to affect cybersecurity;
o) supply chain - the circuit from the manufacturer to the final beneficiary, including the design, development, production, integration, implementation, configuration, use and disposal of software or hardware products and services, respectively networks and information systems;
p) cybersecurity incident management - the set of processes that provide for the detection, qualification, reporting, analysis and response to cybersecurity incidents;
q) cybersecurity risk management - organizational and programmatic strategy involving cybersecurity risk assessment and management activities;
r) management of supply-chain specific cybersecurity risks - organizational and programmatic strategy involving risk assessment and management activities within the processes throughout the life cycle of the software or hardware good or service, respectively the information system or network, from the manufacturer to the final beneficiary, including design, development, production, integration, implementation,

configuration, use and disposal of software or hardware products and services, respectively networks and information systems;
s) cybersecurity policies - general principles and rules needed to be applied to ensure the security of network and information systems;
t) cybersecurity product - as defined in art. 2 lit. l) of Government Emergency Ordinance no. 104/2021, approved with amendments and additions by Law no. 11/2022, as amended;
u) networks and information systems - as defined in art. 3 lit. l) of the Law no. 362/2018 on ensuring a high common level of security of network and information systems, as subsequently amended and supplemented;
v) national defense-specific networks and information systems - the networks and information systems belonging to the Ministry of National Defense, the national networks and information systems supporting the military activities of the North Atlantic Treaty Organization, hereinafter referred to as NATO, and the European Union, hereinafter referred to as the EU, as well as the networks and information systems of interest for national defense given under the responsibility or made available to the Ministry of National Defense in case of armed aggression, when establishing the state of siege, declaration of mobilization or state of war;
w) cyberspace resilience - the ability of a network or information system to withstand a cyber incident or attack and return to the normal state before the cyber incident or attack;
x) cybersecurity risk - as defined in Article 2 paragraph r) of Government Emergency Ordinance no. 89/2022;
y) cybersecurity - normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of electronic information of public or private resources and services in cyberspace;
z) cyberspace - the virtual environment generated by computer networks and systems, including information content processed, stored or transmitted, as well as the actions carried out by users in it;
aa) cybersecurity vulnerability - weakness in the design, implementation, development, configuration and maintenance of network and information systems or related security measures that can be exploited by a threat.

ARTICLE 3
(1) In the field of cybersecurity, this law applies to the following:
a) networks and information systems owned, organized, administered, used or under the competence of public authorities and institutions in the field of defense, public order, national security, justice, emergency situations, National Registry of State Secret Information Office;
b) networks and information systems owned by natural and legal persons under private law and used for the provision of electronic communications services to central and local public administration authorities and institutions;
(c) networks and information systems owned, organized, operated or operated by authorities and institutions of central and local public administration other than those referred to in (a), as well as by natural and legal persons providing public services or services of public interest other than those referred to in (b).

(2) In the field of cyber defense, the purpose of this law is to establish the general regulatory framework for national defense specific networks and information systems.

ARTICLE 4
The objectives of this law are:

a) ensuring the resilience and protection of networks and information systems supporting defense, national security, public order and governance functions;

(b) designating competent authorities and the establishment of the legal framework for the development of capabilities required to fulfill their responsibilities in the areas of cyber security and defense;

c) maintaining or restoring the cybersecurity climate at national level, through cooperation between competent authorities and ensuring the unitary coordination by the Cybersecurity Operational Council, hereinafter referred to as COSC, of the legal entities responsible for their cybersecurity and ensuring a rapid and efficient response to threats arising from cyberspace;

d) establishing and separating functional responsibilities and/or tasks between network providers, information systems and services, law enforcement authorities, structures within institutions responsible for cyber security and defense, so as to ensure a high level of cybersecurity at national level;

e) developing and strengthening a cybersecurity culture at national level, by raising awareness of vulnerabilities, risks and threats, respectively the formation of a proactive and preventive conduct.

ARTICLE 5
Cyber security and defense assurance shall be carried out in accordance with the following principles:

a) personality principle - the responsibility of ensuring cybersecurity and/or cyber defense of a system, network and/or information service lies with the natural or legal person who owns, organizes, manages and/or uses them, as appropriate;

b) the principle of full protection - the natural or legal person responsible for the cyber security and/or defense of an information system, network and/or service is responsible for the management of the risks associated with them and their connections with other third-party information systems, networks and/or services, as well as for the implementation of the technical and organizational measures necessary for cyber protection;

c) the principle of minimization of effects - in case of a cybersecurity incident, the natural or legal person responsible for the cybersecurity and/or cyber defense of the system, network and/or information service in question takes measures to avoid amplification of effects and to extend them to other systems, networks and/or information services under their own responsibility or under the responsibility of other natural or legal persons;

d) the principle of collaboration, cooperation and coordination - consists in the joint implementation by the responsible natural or legal persons of all activities to ensure the security and/or defense of the information systems, networks and services covered by this law, as well as the management of cybersecurity incidents, mitigating the effects and eliminating the situations that generated the states of cyber alert established at national level.

CHAPTER. II
National cybersecurity system
ARTICLE 6
1. For the purpose of organizing and carrying out in a uniform manner at national level activities specific to cybersecurity, the National

Cybersecurity System, hereinafter referred to as the SNSC, shall be established as the general framework for cooperation bringing together the authorities referred to in Article 10 paragraph. (1) as well as other public authorities and institutions with responsibilities and capabilities in the fields of application of this law, with a view to coordinating actions at national level to ensure cybersecurity.
(2) In exercising their powers, the institutions and public authorities referred to in paragraph 1. cooperate with the private sector, academia, professional associations and non-governmental organizations.

ARTICLE 7
(1) The activities of the SNSC are coordinated at strategic level by the Supreme Council of National Defense, hereinafter referred to as the CSAT.
2. The activities of the SNSC shall be coordinated by the COSC at operational level on a uniform basis.
(3) The Romanian Intelligence Service, hereinafter referred to as SRI, provides the technical secretariat of COSC, under the terms of this law.

ARTICLE 8
(1) The COSC is an advisory body, without legal personality, in the coordination of the CSAT, consisting of the Presidential Adviser for National Security, the Prime Minister's Adviser for National Security, the Secretary of the CSAT, and representatives of: the Ministry of National Defense, hereinafter referred to as the MApN, the Ministry of Internal Affairs, hereinafter referred to as the MAI, the Ministry of Foreign Affairs, hereinafter referred to as the MAE, the Ministry of Research, Innovation and Digitization, hereinafter referred to as the MCID, the SRI, the Foreign Intelligence Service, hereinafter referred to as the SIE, the Special Telecommunications Service, hereinafter referred to as the STS, the Protection and Guard Service, hereinafter referred to as SPP, the Office of the National Register of State Secret Information, hereinafter referred to as ORNISS, the National Authority for Management and Regulation in Communications, hereinafter referred to as ANCOM, and the National Cybersecurity Directorate, hereinafter referred to as DNSC.
2. The COSC shall issue consultative opinions and recommendations, adopted by consensus, which shall be addressed to the authorities referred to in paragraph (1), according to legal competence.
(3) The management of the COSC shall be provided by a Chairman - the Presidential Counselor for National Security Matters and a Deputy Chairman - the Prime Minister's Counselor for National Security Matters.
(4) Depending on the nature and evolution of cyber threats, representatives of other entities - authorities, public institutions, legal entities governed by public or private law - that can contribute to solving cyber security issues - are invited to participate in COSC meetings, without voting rights.
(5) The COSC shall be convened by its chairman, at the proposal of any of the members referred to in paragraph. 1.

ARTICLE 9
1. In the performance of its tasks, the COSC shall analyze and evaluate cybersecurity and submit to the CSAT or the DNSC, as appropriate, proposals and briefings on:
a) harmonize the reaction of the competent authorities of the state in situations caused by cyber threats, which require changing the level of cyber alert;
(b) requesting, where necessary, assistance from other States or international organizations and bodies;

c) the manner of responding to requests for assistance addressed to Romania from other states or international organizations and bodies other than those in the field of national defense;
d) plans or directions of action, depending on the resulting conclusions and the evolution of the security climate in cyberspace;
e) directions for development and investment in the field of cybersecurity;
f) mandate lines regarding the adoption of any documents on cybersecurity at international level, which have an impact at national level;
g) ways to manage and respond to cyber threats and attacks.
2. In the exercise of its tasks, the COSC shall inform the CSAT about recommendations and opinions on the establishment or modification of national cyber alert levels.
3. In order to achieve cybersecurity, the COSC shall cooperate, as appropriate, with coordination or management bodies set up at national level for emergency management, crisis actions in the field of public order, prevention and fight against terrorism, national security and defense.

CHAPTER III
Competent authorities and responsibilities
ARTICLE 10
(1) The following are competent authorities within the meaning of this Law:
a) DNSC, for civil national cyberspace, according to the provisions of this law and of the Government Emergency Ordinance no. 104/2021, approved with amendments and additions by Law no. 11/2022, as amended;
b) MCID, for the development and initiation of national legislation and national public policies in the field of cybersecurity, digital transformation, information society, communications, research, development and innovation;
(c) ANCOM, for the coordination of the activities carried out in order to ensure the cyber security of its own network and information systems and those referred to in Article 3(b). (1) (b);
(d) MApN, MAI, MAE, SRI, SIE, STS, SPP and ORNISS, in accordance with the powers laid down in Articles 11 to 18.

(2) The authorities referred to in par. (1) are required to:
a) adopt action plans corresponding to each level of cyber alert;
b) to provide support, within the scope of their duties, at the request of network and information system owners within their remit, activity or responsibility, for the implementation of measures appropriate to cyber alert levels;
c) to carry out information and communication activities to the public, within the scope of their duties;
d) to organize training and training sessions in the field of cybersecurity, within the scope of their tasks;
e) organize or participate in national cybersecurity exercises;
f) to communicate to each other data of interest related to cybersecurity, including to other public authorities and institutions that own, organize, manage, use or have competence in IT networks and systems.

(3) The authorities referred to in par. (1) may develop strategies and rules of their own, through administrative acts of the heads of authorities, for regulating cybersecurity activities at institutional level.

ARTICLE 11
The MApN is the competent authority at national level in the field of cyber defense and for the purpose of this law it has tasks in the field of cyber security for the IT networks and systems that support the military defense capabilities.

ARTICLE 12
MAI, through the specialized structure, is the competent authority at national level in the field of cybersecurity for the knowledge, prevention, identification and counteraction of cyber threats, vulnerabilities and risks to information systems, communication networks and electronic services in the field of competence.

ARTICLE 13
(1) MAE is the competent authority at national level in the field of cyber diplomacy, for ensuring the diplomatic composition and international relations on matters of cyber security, and performs the following tasks:
a) ensures and coordinates the representation of Romania's interests within the international negotiation and political dialog formats to which Romania is a party and whose object of activity can produce national and international implications in terms of rules, principles and rules for the use of information and telecommunications technologies and parameters of responsible state conduct in cyberspace;
b) Supports and promotes strategic cooperation and coordination, as well as Romania's dialog in the field of cyber security and defense with key international partners, both bilaterally and within the international formats to which Romania is a party, as well as on policy decisions with national and international implications on cyberspace;
c) Promote and contribute to the understanding, ownership and application at national and international level of the principles, rules and norms of responsible behavior in cyberspace agreed at UN level, the application of the relevant international law and the use of the cyber diplomacy toolkit at EU level;
d) promote Romania's interests internationally in a manner consistent with the national framework of democratic values and Romania's membership in the North Atlantic Alliance (NATO) and the European Union (EU), by supporting and protecting the global, open, free, stable and secure character of the cyberspace, the full applicability of international law - including international humanitarian law and international human rights law - in this respect, as well as full compliance with the rules of responsible conduct of states in cyberspace agreed in the ONU system, in order to maintaining stability, preventing conflicts and mitigating cyber threats.
(2) MAE shall cooperate with the COSC member authorities, in particular with a view to:
a) ensuring the diplomatic composition of cybersecurity;
b) promoting uniformly Romania's interests and a coherent message in Romania's external action;
c) participation in the cybersecurity ecosystem at international level;
d) to ensure a unified and timely response in the external policy approach to new developments and situations in the field of cybersecurity that may have consequences for cyber security and defense.

ARTICLE 14
(1) SRI is the competent authority at national level in the field of cyber intelligence, as well as for the knowledge, analysis, prevention

and counteraction of cyber incidents and attacks that represent threats, risks and vulnerabilities to the national security of Romania.
(2) Preventing and combating APT- type threats to networks and information systems in the field of competence, activity or responsibility, as the case may be, of the institutions and authorities referred to in Article 10 paragraph (1) the following shall be done:
(a) by the MApN within the powers laid down in Article 11;
(b) by the MAI within the powers laid down in Article 12;
(c) by the SIE within the powers laid down in Article 15;
(d) by the STS within the powers laid down in Article 16;
(e) by the SPP within the powers laid down in Article 17;
(f) by the SRI, in all other cases.
(3) In the case of cyber threats to the network and information systems referred to in Article 3. (1) paragraphs b) and c), which would prejudice national security, SRI informs ANCOM and DNSC, under the law.

ARTICLE 15
The Foreign Intelligence Service (SIE) is the competent authority for documenting, analyzing, preventing and countering cyber incidents and attacks that represent cyber threats, risks and vulnerabilities to network and information systems under its responsibility.

ARTICLE 16
STS is the competent authority in the field of cybersecurity for its own infrastructure, networks, systems, services and radio spectrum, as well as for those regulated by special laws.

ARTICLE 17
SPP is the competent authority in the field of cybersecurity for its infrastructure, networks, systems and services, coordinates cybersecurity measures for the dignitaries it protects and acts, independently or in cooperation with other structures in the fields of defense, public order and national security, to implement them.

ARTICLE 18
ORNISS coordinates the activities carried out in order to ensure the cyber security of network and information systems that store, process or transmit classified information, according to the tasks set out in Government Emergency Ordinance no. 153/2002 on the organization and functioning of the National Register of State Secret Information Office, approved by Law no. 101/2003, with subsequent amendments and additions.

ARTICLE 19
(1) The authorities referred to in Article 10 shall set up and operate dedicated cybersecurity audit facilities and dedicated cybersecurity structures for the management of cyber threats to computer networks and systems under their responsibility.
(2) The structures referred to in para. (1) the head of the authorities referred to in Article 10 shall be established, organized and operated by administrative act.

CHAPTER IV
Incident management and resilience in cyberspace
SECTION 1
Cybersecurity incident management

ARTICLE 20
(1) DNSC shall develop and ensure the management of the National Cybersecurity Incident Reporting Platform, hereinafter referred to as PNRISC.
(2) The authorities referred to in Article 10 shall have access to the PNRISC for the performance of their responsibilities.
(3) The processing of the information from the PNRISC is carried out in compliance with the confidentiality and transparency policies established and implemented by the DNSC.

ARTICLE 21
(1) The persons referred to in Article 3 (1) paragraph b) and c) are required to notify cybersecurity incidents through the PNRISC immediately, but no later than 48 hours after the incident is detected.
(2) If cybersecurity incidents cannot be fully communicated within the period stipulated in para. (1), they shall be sent no later than 5 calendar days after the initial notification, the information may be supplemented and subsequently with the information arising from the investigations conducted on the basis of the event.
(3) Without prejudice to the applicable rules concerning reporting, confidentiality, professional secrecy and protection of classified information, the authorities responsible for the networks and information systems referred to in Article 3 para. (1) paragraph a) notifies cybersecurity incidents via the PNRISC.

ARTICLE 22
Cybersecurity incidents are notified in the PNRISC under the conditions of Section 2 of Chapter IV of Law No 362/2018, as amended and supplemented.

ARTICLE 23
In the field of management of cybersecurity incidents, the authorities referred to in Article 10 para. (1) points (c) and (d) shall have the following responsibilities:
a) to collect notifications of cybersecurity incidents within IT networks and systems in their area of competence, activity or responsibility;
b) to assess data and information on cyber incidents and attacks against network and information systems in their area of competence, activity or responsibility;
(c) to coordinate the management of cybersecurity incidents identified within computer networks and systems in their area of competence, activity or responsibility;
d) to provide support, upon request, to owners, administrators, owners and/or users of networks and information systems falling within their remit, activity or responsibility, for the adoption of emergency reactive measures to remedy the effects of cybersecurity incidents;
e) to keep for 5 years the data on cybersecurity incidents and the results of measures to counter them, without collecting content data.

SECTION 2
Resilience in cyberspace
ARTICLE 24
(1) Ensuring resilience in cyberspace shall be achieved through the implementation of proactive and reactive measures by the institutions and individuals referred to in Article 3.

(2) Proactive measures shall be aimed at preventing cybersecurity incidents and deterring perpetrators of cyberspace attacks and shall include:

a) setting up and training cybersecurity incident response teams;

b) providing specialized human resources for the development of strategies, rules, policies, procedures, risk analysis, plans and technical control measures on defense and cyber security;

c) the establishment and operation of operational security centers;

d) the establishment of a pool of resources and capabilities met by cybersecurity that can be used in case of need;

e) development of proactive capabilities, allowing for the anticipatory knowledge of threats in cyberspace;

f) funding for the development of cyber security and defense capabilities, including from the perspective of research, development, innovation and digitalization in the field and uptake of emerging technologies;

g) cooperation and exchange of information between competent authorities and the private sector for the identification of cyber threats;

h) identifying IT services, networks and systems, in accordance with the competences of each institution responsible for their management and ensuring their management;

i) implementation of cybersecurity solutions that increase detection capacity and cyber-attack prevention capabilities;

j) developing strategies, rules, policies, procedures, risk analysis, plans and technical control measures on defense and cyber security;

k) demonstrating the level of maturity achieved by cybersecurity capabilities in exercises organized at national or international level;

l) training of staff of persons referred to in Article 3 in the field of cybersecurity, through regular information, awareness and cyber-hygiene campaigns at organizational level.

(3) Reactive measures shall be aimed at reducing the effects of cyber-attacks and shall include:

a) implementing incident response and contingency plans in the field of cybersecurity;

b) the use of the reserve of cybersecurity resources and capabilities;

c) restoring the functionality of network and information systems within the affected institutions;

d) disseminating information about cyber events through alerts in the interinstitutional environment to assess the risk and reduce the possibilities of exploiting vulnerabilities;

e) discouraging through public attribution of the perpetrators of cyber attacks, according to the legal powers.

ARTICLE 25

(1) Providers of technical cybersecurity services shall, at their reasoned request, make available to the authorities referred to in Article 10, within a maximum of 48 hours from the date of receipt of the request, data and information on incidents and within a maximum of 5 days from the date of receipt of the request, on threats, risks or vulnerabilities the manifestation of which may affect a network or information system as referred to in Article 3 para. (1) and their interconnection with third parties and end-users.

(2) The data and information referred to in para. (1) does not concern personal data and content data for the purpose of the request.

(3) The data and information referred to in para. (1) shall be transmitted in writing, by electronic means or by any other mutually agreed means, in the format and structure consistent with the reporting of cyber incidents in the PNRIS, referred to in Article 22.

ARTICLE 26
In order to increase the level of cyber resilience and achieve deterrence in cyberspace at national level, DNSC and institutions in the fields of defense, public order and national security shall take measures to:

a) the implementation of an interinstitutional cybersecurity framework allowing joint training, knowledge transfer, information exchange, expert support and federation of cybersecurity resources and capabilities;

b) improving and expanding the capabilities of automatic attack protection and detection, by implementing tools for intelligent threat analysis and timely distribution of indicators and warnings of impending cyber-attacks on national network and information systems;

c) developing manuals with techniques, tactics and procedures as well as contingency plans and exercising them in cybersecurity exercises in order to strengthen resilience in cyberspace;

d) the setting up of computer security incident response team, hereinafter referred to as CSIRT, cyber protection teams and/or other forces specialized in the deployment of actions in cyberspace.

CHAPTER V
National Cyber Alert System
ARTICLE 27
(1) The National Cyber Alert System, hereinafter referred to as SNAC, consists of a set of technical and procedural measures aimed at preventing, deterring and combating actions or inactions that may constitute vulnerabilities, risks or threats to Romania's cyber security.
(2) The SNAC shall provide a service of public notification of the existing national level of cyber alert, for a defined geographical area or area of activity, determined by the degree of risk associated with the identified threats to cyber incidents or attacks at a given time.

ARTICLE 28
(1) Cyber alert levels and lines of action in cyber alert situations shall be established by a methodology developed by the DNSC, endorsed in accordance with the COSC and approved by order of the DNSC Director.
(2) The setting of alert levels and the transition from one level to another shall be decided by the Director of the DNSC, with prior advisory opinion or on a proposal from the COSC, as appropriate.
(3) The transition from a higher to a lower level of cyber alert shall be done after the cessation of the causes that led to the raising of the alert level.

ARTICLE 29
(1) The persons referred to in Article 3 shall be required to draw up their own action plans for each type of cyber alert in

accordance with the methodology laid down in Article 28, paragraph (1).

(2) When declaring states of cyber alert, the persons referred to in Article 3 shall implement the measures in the plans referred to in paragraph (1)

CHAPTER VI

Cyber Defense

ARTICLE 30

(1) In the field of cyber defense, the MApN shall have the following tasks:

a) defends and protects the MApN's computer systems and networks;

b) plan and conduct operations in cyberspace through the National Military Command Center, according to the law;

c) plan and execute defensive operations in cyberspace in peacetime through the Cyber Defense Command;

d) develop and implement military capabilities for the execution of operations in cyberspace through the Cyber Defense Command;

e) conducts cyber intelligence and cyber counter-intelligence operations in cyberspace for the purpose of knowing, monitoring and countering threats to national defense, to the MApN structures and to the allied forces;

f) develop offensive response capabilities, individually or as part of a coalition or alliance, usable in case of cyber-attacks that are contrary to international law;

g) participates in deterrent activities in cyberspace;

h) provide the single point of contact with NATO for military operations in cyberspace;

i) develop and implement policies and standards in the field of cyber defense, in accordance with the national interest, as well as with the standards and requirements stemming from Romania's accession to NATO, the EU and the Organization for Economic Cooperation and Development.

(2) The MApN shall cooperate with the other structures within the national defense, public order and national security system to ensure the cyber defense of network and information systems within their area of competence, activity or responsibility.

(3) The cyber defense activities and operations in cyberspace, the development of offensive response capabilities and deterrent activities in cyberspace referred to in paragraph 1 shall be organized, planned and conducted in compliance with international law, including international humanitarian law, the rules of responsible conduct of states in cyberspace agreed in the UN system, as well as the other treaties to which Romania is a party.

ARTICLE 31

The MApN sets out, through the Government's decision, the concrete conditions for recruitment/selection, the arrangements for regular training and training, the incentives of legal entities under private law, as well as the conditions for establishing and using the reserve of cyber defense specialists.

CHAPTER VII

Cybersecurity research, development and innovation

ARTICLE 32

(1) Research, development and innovation in the field of cybersecurity are an integral part of the national research,

development and innovation system and are aligned with the measures promoted by the MCID for framing the Romanian research area in the European Research Area.

(2) The MCID shall develop a multi-annual program for the financing of cybersecurity research, development and innovation projects, in which public and private research organizations as well as public authorities and institutions with tasks in the field of cybersecurity may participate.

(3) By way of derogation from Article 30 paragraph (2) of the Law on fiscal responsibility No 69/2010, republished, as subsequently amended and supplemented, the annual budget allocated to the program referred to in paragraph (2) shall be at least 10 % of the budget allocated to the research programs financed by the MCID for that year.

(4) The financing for the program referred to in paragraph (2) shall be carried out on transparent and competitive criteria, according to a competition methodology adopted by order of the Minister for Research, Innovation and Digitization, published in the Official Gazette of Romania, Part I.

ARTICLE 33

(1) The authorities referred to in Article 10 shall develop their own strategies and policies for research, development and innovation in the areas of cyber security and defense, according to their scientific potential, specific skills or missions.

(2) At the level of each authority referred to in Article 10, the head of the institution shall designate the entity responsible for the management of research, development and innovation activities in the fields of cyber security and defense.

(3) The authorities referred to in Article 10 shall cooperate with academia, industry and the European Cybersecurity Industrial, Technology and Research Competence Center, as well as with the Network of National Coordination Centers, in implementing the following lines of effort in the field of research, development, innovation and digitization:

(a) maintaining an advanced position among institutions investing and capitalizing on the results of research, development and innovation activities carried out in the field of cybersecurity;

(b) developing and maintaining effective partnerships in the field of research, development, innovation and digitalization;

(c) promoting new technologies, prototypes and technological demonstrators in the fields of cyber security and defense;

(d) the development of networks of experts in the field at national and interinstitutional level.

CHAPTER VIII
Cooperation in cyber security and defense
SECTION 1
At national level

ARTICLE 34

(1) Cooperation in the field of cyber security and defense at national level shall have the following objectives:

(a) achieving a dynamic and efficient response to cybersecurity incidents;

(b) building on experience and best practices in the areas of cyber security and defense;
(c) implementing an open, transparent, collaborative and trusted environment between institutions with responsibilities in the field of cyber security and defense at national level;
(d) acceptance and promotion of cybersecurity standards in partnership with the national industry;
(e) development and implementation of cybersecurity solutions by all public authorities and institutions;
(f) developing a culture of cybersecurity and implementing good cyber hygiene practices at national level;
(g) ensuring coordinated and unified public communication, where the situation requires, in the context of cyber-alert situations, cyber-attacks with significant impact or emerging threats from cyberspace;
(h) situational awareness and communication to the public of measures recommended for implementation, with a view to facilitating cyber crisis management.
(2) Cooperation activities at national level shall include at least the following:
(a) development of cyber security and defense capabilities;
(b) reporting of cyber incidents and cooperation in cyber-alert situations;
(c) research, development, innovation and digitization programs;
(d) training or specialization courses;
(e) cybersecurity exercises;
(f) conferences and other scientific events.

SECTION 2
At international level
ARTICLE 35
International cooperation in the fields of cyber security and defense shall have the following objectives:
(a) mutual information on threats in cyberspace;
(b) increasing the responsiveness to cyber threats and building cohesion of action by specialized teams in multinational cyber security and defense exercises;
(c) verifying and validating the level of maturity achieved by cyber security and defense capabilities implemented at national level;
(d) achieving technical and procedural interoperability of cyber defense forces;
(e) achieving technical and procedural interoperability of cyber defense forces;
(f) the development of joint research, development and innovation projects in the fields of cyber security and defense;
(g) evaluating and implementing revolutionary cybersecurity solutions and adopting new concepts for the design and use of emerging technologies in cyberspace;
(h) increasing national contribution to knowledge transfer, confidence-building and capacity-building activities in the field of cyber security and defense;
(i) representing Romania's interests in international negotiation and dialog formats whose object of activity may produce national and international implications in terms of rules, principles and rules for the use of information and telecommunications technologies and parameters of responsible state conduct in cyberspace, as well as in joint actions with strategic partners and

at NATO and EU level in the application of cyber diplomacy tools to deter cyber-attacks, threats, risks and vulnerabilities at international level.

ARTICLE 36

(1) The authorities referred to in Article 10 shall cooperate with the authorities and institutions of the Member States, EU and NATO bodies, agencies and institutions responsible for cyber security and defense, including authorities and institutions of other partner States, in accordance with their respective areas of competence.

(2) Cooperation in the field of cyber defense with NATO institutions, with the armies of EU member countries and allied states is achieved through the MApN.

(3) Cooperation in the field of cyber defense with NATO institutions, with the armies of EU member countries and allied states is achieved through the MApN.

(4) in order to ensure coordination and interinstitutional dialog with a view to ensuring adequate representation and a coherent message in Romania's external action, as well as for the realization of the tasks referred to in Article 13, the activities referred to in paragraph 1 shall be carried out in cooperation with MAE.

CHAPTER IX

Vocational training, education, training

ARTICLE 37

The persons referred to in Article 3 shall be required to provide for their staff the training, education and training in cyber security and defense through courses, exercises, conferences, seminars and other activities.

ARTICLE 38

(1) Defense, public order and national security authorities and institutions may organize, at institutional or interinstitutional level, cyber security and defense exercises.

(2) The authorities and institutions referred to in paragraph (1) shall draw up and adopt an annual and multi-annual plan of cyber security and defense exercises.

ARTICLE 39

(1) Authorities and institutions in the fields of defense, public order and national security participate in cyber security and defense exercises organized at international level, respectively at EU and NATO level.

(2) Participation in cyber defense exercises organized within NATO is carried out under the coordination of the MApN.

ARTICLE 40

The DNSC and the authorities and institutions in the fields of defense, public order and national security shall have the following tasks:

a) ensure the information and training at national level of the population, as well as of all natural and legal persons acting in the national cyberspace, including economic operators in the sectors established according to the provisions of Law 362/2018, as amended and supplemented, and in the public sector on the identified cybersecurity risks, threats and vulnerabilities;

b) promote the development of responsible behavior in cyberspace for natural and legal persons by raising awareness of the effects of cyber-attacks and how to report them;

c) provide information on the obligations arising from the ownership, administrator, organizer, provider or user of information networks and systems, on the attitude to possible cyber-attacks, on the awareness of citizens and public and private institutions, on the need to report/notify cyber-attacks;

d) the development of the national population awareness framework in cooperation with the public, private and academic environment, in order to prepare the population regarding the ways of behavior, reaction and defense in the online environment.

e) carry out and participate in campaigns/actions to prevent and raise awareness of the causes and consequences of cyber-attacks on civil information networks and systems at international, national and regional level.

CHAPTER.X Security of the supply chain

ARTICLE 41

(1) The persons referred to in Article 3 shall implement the supply chain specific cybersecurity risk management processes, in accordance with the provisions of Article 52 para. 1.

(2) The supply chain risks shall include at least the following:

a) delivery of false or counterfeit IT solutions;

b) unauthorized production;

c) fraudulent manipulation of software and hardware products and services, and of information systems and networks;

d) insertion of false or counterfeit software and hardware;

e) software and hardware services dangerous for operation;

f) cyber espionage;

g) unintended compromises in IT systems and networks;

h) poor manufacturing practices and software and hardware development.

ARTICLE 42

The persons referred to in Article 3 shall appoint cybersecurity officers, in accordance with Article 52 para. 1 in the case of:

a) establishing supply chain specific cybersecurity risk management policies, strategies and processes;

b) including in the content of existing policies, strategies and processes new and emerging requirements on supply-chain specific cyber risk management;

c) establishing mandatory cybersecurity risk management standards for contracting authorities in procurement procedures;

d) establishing incentives for potential suppliers in procurement processes, in relation to the level of implementation of their cybersecurity practices;

e) establishing methodologies and applications used to assess supply-chain-specific cybersecurity risks;

f) exchange information with other institutions on supply chain-specific cyber threats, risks and vulnerabilities;

g) developing the methodology for assessing the level of maturity and the ability of supply chain operators to perform cybersecurity risk management;

h) collecting and updating data on the efficiency of providers in eliminating or mitigating cybersecurity risks.

ARTICLE 43

The persons referred to in Article 3 shall arrange for the organization of training courses in the field of supply chain specific cybersecurity risk management, i.e. the introduction of new topics within existing training courses and programs.

ARTICLE 44

Persons referred to in Article 3 may develop advanced cybersecurity risk testing and assessment capabilities to identify cybersecurity vulnerabilities of equipment, software or component parts purchased or developed at institutional level.

CHAPTER XI

Confidentiality and protection of data and information security for natural and legal persons

ARTICLE45

(1) The authorities referred to in Article 10 who request and receive data and information from any natural and legal person under this Law shall take appropriate measures to protect their security and commercial interests, the persons supplying such data and information, and the persons to whom such data and information relate.
(2)The transmission of data and information obtained under this Law from any natural and legal person governed by private law may be carried out only for the performance of the legal duties of the authorities and institutions which obtain such data and information, with the guarantee of the confidentiality of personal data and the protection of the interests and business secrets of natural and legal persons governed by private law.

ARTICLE 46

(1) The processing of personal data falling within the scope of this law shall be carried out in compliance with the legal regulations on the protection of individuals with regard to the processing of personal data.
(2) Notifications under this law shall not affect the obligations of the controllers of personal data established pursuant to Articles 33 and 34 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
(3) For the purpose of carrying out the tasks or provisioning the services provided for by this law, as well as for the purpose of preventing and responding to cybersecurity incidents or for cooperation at national, Community and international level in preventing and responding to cybersecurity incidents, the authorities provided article 10 collects, receives, processes and transmits data and information which may constitute or contain personal data, within the limits of the applicable legislation, with the assurance of compliance with the provisions of par. 2.

ARTICLE 47

(1) This law does not affect national legislation on the protection of personal data, in particular Law No 506/2004 on the processing of personal data and on the protection of privacy in the electronic communications sector, as amended and supplemented, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning

the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Law No 190/2018 on measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 200 16 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as amended.
(2) This law respects the fundamental rights and observes the principles recognized in particular by the Charter of Fundamental Rights of the European Union, including the right to respect for private and family life, the right to the protection of personal data, the right to property and the integration of persons with disabilities, so that nothing in this law must be interpreted or implemented in a manner inconsistent with the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

CHAPTER XII
Offenses and sanctions

ARTICLE 48
(1) The following acts constitute contraventions if they have not been committed under such conditions as to be considered offenses under the law:
a) failure of the persons referred to in Article 3 (a) to comply with the provisions of this Regulation; (1) points (b) and (c) of the obligation to notify cybersecurity incidents through the PNRISC, within the time period provided for in Article 21 paragraph. 1.;
b) failure of the persons referred to in Article 3 (a) to comply with the provisions of this Regulation. (1) points (b) and (c) of the obligation to fully communicate cybersecurity incidents through the PNRISC, within the time limit and conditions set out in Article 21 paragraph. (2) and Article 22;
c) failure by cybersecurity service providers to make available to the authorities referred to in article 10 data and information on incidents, threats, risks or vulnerabilities the manifestation of which may affect a network or information system of the holder or of third parties, under the conditions and within the time limit stipulated in article 25 para. 1.
(2) By way of derogation from Article 8 (a) (2) paragraph a) of Government Ordinance no. 2/2001 on the legal regime of contraventions, approved with amendments and additions by Law no. 180/2002, with subsequent amendments and additions, the contraventions provided in par. 1. the following penalties shall be imposed:
a) with a fine from 5.000 lei to 50.000 lei, and in case of a new offense within 6 months, from the date of the first offense, the maximum limit of the fine is 200.000 lei;
b) for economic operators with a net turnover of more than 1.000.000 lei, with a fine of up to 1% of net turnover, and in case of a new offense, within 6 months, from the date of the first offense, the maximum limit of is 3% of net turnover.
(3) The net turnover stipulated in par. (2) point (b) shall be that recorded by the economic operator in the last financial year.
(4) In order to individualize the sanction provided in par. (2), the official establishing and enforcing the offense considers the degree of

concrete social danger of the act and the period of time during which the legal obligation was violated.
and family enterprises, the turnover provided in par. (2) subparagraph (b) corresponds to all the income received by the economic operators concerned in the financial year preceding the penalty.
(6) For the newly established legal entities and for the legal entities that did not register turnover in the financial year prior to the sanction, the fine stipulated in par. 2. shall be set at a minimum of one and a maximum of 25 gross minimum wages per economy.
(7) To the extent that this law does not provide otherwise, the offenses referred to in par. (1) the provisions of Government Ordinance no. 2/2001, approved with amendments and additions by Law no. 180/2002, with subsequent amendments and additions, apply to them.

ARTICLE 49

(1) Finding the offenses referred to in Article 48 para. (1) points a) and b) shall be carried out by the supervisory staff of the DNSC and the application of the corresponding sanction shall be made by decision of the director of the DNSC.
(2) Finding the offenses referred to in Article 48 para. 1. point (c) shall be carried out by the control staff specifically designated from the authorities referred to in Article 10, corresponding to the authority which made the request for the making available of the information and data, and the application of the appropriate sanction shall be made by administrative act of the control staff specifically designated and delegated by the head of the authority.
(3) The administrative acts referred to in paragraph (1) and (2) must contain the following elements:
a) the identification data of the offender;
(b) the date on which the act was committed;
(c) a description of the offense and the circumstances which have been considered in the individualization of the penalty;
(d) an indication of the legal basis on which the infringement is established and penalized;
(e) the penalty imposed;
(f) the time limit and the method of payment of the fine;
g) the time limit for appeal and the competent court.
(4) By way of derogation from the provisions of Article 13 of Government Ordinance no. 2/2001, approved with amendments and additions by Law no. 180/2002, with subsequent amendments and additions, the application of the sanction referred to in Article 48 para. (2) shall be statute barred within one year from the date on which the act was committed. In the case of time-consuming infringements or infringements consisting in the commission, on the basis of the same resolution, at different intervals of time, of several acts or omissions, each of which contains the content of the same offense, limitation shall begin to run from the date of the finding or the date of the termination of the last act or fact, whichever is the earlier.
(5) By way of derogation from the provisions of Article 25 par. (2) from Government Ordinance no. 2/2001, approved with amendments and additions by Law no. 180/2002, with subsequent amendments and additions, the administrative act stipulated in par. (1) or (2) shall be notified to the offender within 15 days from the date of issue.
(6) At the same time as the administrative act stipulated in par. (1) or (2), the offender shall also be notified of the payment notice, which

shall state that the fine must be paid within 30 days of the date of notification of the act.
(7) The administrative act referred to in par. (1) or (2), not challenged within the time limit stipulated in par. (9) as well as the final court decision on the administrative action shall be enforceable without any further formality. The action in administrative contentious cases under the conditions stipulated in par. 9. suspend enforcement only in respect of the payment of the fine until the court has given a final judgment.
8. The amounts of the fines imposed under this Article shall be paid in full to the State budget. Enforcement shall be carried out in accordance with the legal provisions on enforced execution of tax claims. In order to enforce the sanction, the DNSC and the authorities referred to in Article 10 shall communicate of their own motion to the specialized bodies of the National Revenue Agency the administrative act referred to in paragraph. (1) or (2), not challenged within the time limit stipulated in par. (9) after the expiry of the period provided for in the payment notice or after the final decision on the administrative appeal has become final.
(9) By way of derogation from the provisions of Article 7 of the Law on Administrative Litigation No 554/2004, as subsequently amended and supplemented, and from the provisions of Article 32 par. (1) from Government Ordinance no. 2/2001, approved with amendments and additions by Law no. 180/2002, with subsequent amendments and additions, administrative acts and decisions adopted according to the provisions of this law can be appealed in administrative proceedings at the Bucharest Court of Appeal, without the prior procedure, within 30 days from their communication.
(9) By way of derogation from the provisions of Article 7 of the Law on Administrative Litigation No 554/2004, as subsequently amended and supplemented, and from the provisions of Article 32 para. (1) from Government Ordinance no. 2/2001, approved with amendments and additions by Law no. 180/2002, with subsequent amendments and additions, administrative acts and decisions adopted according to the provisions of this law can be appealed in administrative proceedings at the Bucharest Court of Appeal, without the prior procedure, within 30 days from their communication.
(10) By way of derogation from Article 14 para. (1) of Government Ordinance no. 2/2001, approved with amendments and additions by Law no. 180/2002, with subsequent amendments and additions, the execution of the administrative sanctions applied is time-barred if the administrative act stipulated in para. (1) or (2) has not been communicated to the offender within 15 days from the date of application of the sanction.

CHAPTER XIII
Provisions regarding the completion of art. 3 of the Law no. 51/1991 on the national security of Romania, republished, with subsequent amendments and additions, as well as for the modification of the Government Emergency Ordinance no. 1/1999 on the regime of the state of siege and the regime of the state of emergency, approved with amendments and additions by Law no. 453/2004, with subsequent amendments and additions.

ARTICLE 50
In Article 3 of Law 51/1991 on National Security of Romania, republished in the Official Gazette of Romania, Part I, no. 190 of 18 March 2014, as amended and supplemented, three new paragraphs (n) to (p) are inserted after the paragraph m), which reads as follows:

‘’(n) cyber threats or cyber attacks on information and communication infrastructure of national interest;
o) actions, inactions or facts with consequences at national, regional or global level that affect the state's resilience to hybrid risks and threats;
p) actions carried out by a state or non-state entity, by carrying out, in cyberspace, propaganda or disinformation campaigns, such as to affect constitutional order.’’

ARTICLE 51
Government Emergency Ordinance no. 1/1999 on the curfew regime and the emergency state regime, published in the Official Gazette of Romania, Part I, no. 22 of January 21, 1999, approved with amendments and additions by Law no. 453/2004, with subsequent amendments and completions, is amended as follows:

1. ARTICLE 2 will read as follows:

ARTICLE 2
The state of siege is the set of exceptional measures of a political, military, economic, social and other nature applicable throughout the country or in some administrative-territorial units, established to adapt the country's defense capability, including cyber defense, to serious, current or imminent dangers, which threaten the sovereignty, independence, unity or territorial integrity of the state. Exceptional measures applicable throughout the country or in some administrative-territorial units may be taken in the event of the establishment of a state of siege.

2. ARTICLE 3(a) shall read as follows:
“a) the existence of current or imminent serious threats to Romania's national security, including cyber security for reasons of national security, or the functioning of constitutional democracy;”

3. ARTICLE 23 will read as follows:
“ARTICLE 23
Military orders shall be issued within the limits set by the Decree establishing the exceptional measure, as follows:
1.during curfew:
a) by the Minister of National Defense or the Chief of the General Staff of Defense, when the state of siege has been established throughout the territory of the country;
b) commanders of large units within the territorial range for which they were empowered by the Chief of Defense Staff, when the state of siege was established in certain administrative-territorial units;
2. during the state of emergency:
a) by the Minister of Internal Affairs or his legal substitute, when the state of emergency has been established throughout the country;
b) by the officers empowered by the Minister of Internal Affairs or by their legal replacements, when the state of emergency has been established in certain administrative-territorial units.
(2) In the event of the imposition of the exceptional measure for cases concerning cyber security or defense under the conditions of Articles 2 and 3(a), the issuers of military orders shall seek the prior and advisory opinion of the Cyber Security Operational Council.

CHAPTER XIV
Transitional and final provisions

ARTICLE 52

(1) The categories of persons referred to in Article 3 paragraph (1) paragraph c) shall be established by a Government decision, initiated by the MCID, adopted no later than 60 days after the date of entry into force of this Law.

(2) The administrative provisions referred to in Article 19 (a) (2) shall be issued within 90 days of the date of entry into force of this law.

(3) For the application of the provisions of Article 20 para. (3), confidentiality and transparency policies are issued by order of the Director of DNSC within 90 days from the date of entry into force of this law.

(4) In order to apply the provisions of Article 24, the authorities referred to in Article 10 shall adopt their own cyber resilience measures within a maximum of 120 days from the date of entry into force of this Law.

(5) Methodological rules for requesting and communicating the data and information referred to in Article 25 para. (1) are determined by a Government decision, initiated by the MCID, adopted no later than 90 days after the date of entry into force of this Law.

(6) For the application of the provisions of Article 28 para. (1), the methodology is issued by order of the director of DNSC within 6 months from the date of entry into force of this law.

(7) For the purposes of applying the provisions of Article 31, the Government shall adopt this decision no later than 90 days after the date of entry into force of this Law.

(8) For the purposes of applying the provisions of Article 32 para. (2)-(4), the Minister for Research, Innovation and Digitization shall issue this order no later than 120 days after the date of entry into force of this law.

ARTICLE 53

The provisions of Articles 48 and 49 shall enter into force 30 days after the date of publication of this Law in the Official Gazette of Romania, Part I.

a) This law was adopted by the Romanian Parliament, in compliance with the provisions of art. 75 and art. 76 para. (1) of the Constitution of Romania, republished.