2216

Pursuant to Article 81 of the Constitution of the Republic of Croatia, the Croatian The Council at its session on November 15, 2024, adopted

DECISION

ON THE APPOINTMENT OF A DEPUTY MEMBER DELEGATIONS OF THE CROATIAN PARLIAMENT TO TO THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE

I.

DANIJELA BLAŽANO-VIÿ is hereby appointed as a deputy member of the Delegation of the Croatian Parliament to the Parliamentary Assembly of the Council of Europe.

II.

This Decision will be published in the Official Gazette and will enter into force on the day of its adoption.

Class: 021-04/24-04/11

Zagreb, November 15, 2024.

CROATIAN PARLIAMENT

President
Croatian Parliament
Gordan Jandrokoviÿ, mp

GOVERNMENT OF THE REPUBLIC OF CROATIA

2217

Pursuant to Article 24 of the Cybersecurity Act (Official Gazette, No. 14/24), the Government of the Republic of Croatia, at its session held on 21 November 2024, adopted

REGULATION

ABOUT CYBER SECURITY

PART ONE

GENERAL PROVISIONS

Article 1.

This Regulation regulates the criteria for classifying entities based on special criteria for implementing the categorization of entities, criteria for conducting assessments for the purpose of categorizing public sector entities and entities from the education system, data collection for the purpose of implementing the categorization of entities and maintaining a special register of entities, maintaining a list of key and important entities, maintaining a special register of entities, measures for managing cyber security risks and the method of their implementation, conducting cyber security self-assessments, a form for the declaration of conformity, criteria for determining significant incidents, reporting on significant incidents, other incidents, cyber threats and avoided incidents, access rights and other issues relevant to the use of the national platform for collecting, analyzing and exchanging data on cyber threats and incidents, submitting requests and proposals, collecting data necessary for conducting an assessment of the criticality of entities, as well as other issues relevant to the implementation of the accession of entities to the national system for detecting cyber threats and protecting cyberspace.

Article 2.

The following are an integral part of this Regulation:

– Annex I – List of sectors of activity (hereinafter referred to as: Annex I to this Regulation)

– Annex II. – Cybersecurity risk management measures (hereinafter: Annex II of this Regulation)

– Annex III – Specific physical security measures for entities in the digital infrastructure sector (hereinafter referred to as: Annex III of this Regulation) and

– Annex IV – Form of the declaration of conformity (hereinafter referred to as Annex IV to this Regulation).

Article 3.

This Regulation transposes into Croatian legislation Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning 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 (NIS2 Directive) (OJ L 333/80, 27. 12. 2022).

Article 4.

(1) For the purposes of this Regulation, certain terms have the following meanings:

1. activity is any activity explicitly listed in Annex I and Annex II of the Cybersecurity Act (Official Gazette, No. 14/24; hereinafter referred to as: the Act)

2. Hacktivism involves the use of cyberattacks for the purpose of promoting and encouraging certain political positions or social changes, as well as with the aim of expressing some kind of civil disobedience, and is carried out by organized cyber groups or individuals, who are called hacktivists.

3. indicators of compromise (Indicators of Compromise - IoCs) are data that represent indicators of possible network and information system compromise, which are used for the purpose of detecting and preventing cyberattacks, i.e. with the aim of reducing potential damage by stopping a cyberattack in its earlier stages, and typical indicators of compromise are IP addresses, file names, cryptographic summaries of files, malicious domains and domains of management and control of cyberattackers

4. public media service provider is a media service provider as defined in Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/
EU (European Media Freedom Act) (Text with EEA relevance) (OJ L, 17.4.2024)

5. the competent authorities for the implementation of the categorization of subjects are the competent authorities for the implementation of cyber security requirements and the competent authorities for the implementation of special laws, according to the division of competences from Annex III. of the Law

6. The competent authority for maintaining a special register of entities is the Si-security intelligence agency

7. Obligors to submit data for categorization of entities are
entities from Annexes I and II. of the Law

8. The entities obliged to submit data for maintaining a special register of entities are DNS service providers, the registry of top-level national Internet domain names, registrars, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed

security services, online marketplace providers, internet search engine providers and social networking service platform providers

9. Operational technology (OT) represents a wide range of programmable systems and devices that interact with the physical environment or control other devices that interact with the physical environment and detect or cause direct change in the physical environment through monitoring and/or control of devices, processes and events.

10. persons responsible for the management of cyber security risk management measures are members of management bodies of key and important entities, i.e. heads of state administration bodies, other state bodies and executive bodies of local and regional (regional) units
self-government

11. Service recipient is any natural or legal person to whom a key or important entity provides a service pursuant to law or a service provision contract. A service provision contract is a contract governing the provision and use of a service or other legally binding document governing the legal relationship between the service recipient and the key or important entity as a service provider, including the general terms and conditions of the entity and other pre-written rules by which the entity regulates in advance the legal relationships with the recipients of its services

12. applied scientific research is industrial research, experimental development or a combination thereof. Industrial research is a planned investigation or critical review with the aim of acquiring new knowledge and skills for the development of new products, processes or services or for achieving significant improvements in existing products, processes or services. Experimental development is the acquisition, combination, shaping and use of existing scientific, technological, business and other relevant knowledge and skills for the development of new or improved products, processes or services. Experimental development may include activities aimed at conceptually defining, planning and documenting new products, processes or services.

13. reduced service quality level is the service quality level
which is less than the prescribed or contracted level of service quality

14. The effect on authenticity is the influence on the property that an entity is what it claims to be.

15. impact on integrity is the impact on the property of accuracy and completeness

16. impact on availability is the impact on the continuity of service provision, a reduction in the level of service quality and a partial or complete interruption of service provision.

17. impact on confidentiality is the impact on the availability property in such a way that information is accessible to unauthorized persons, individuals, entities or processes

18. service is any service explicitly listed in Annex I and Annex II of the Act, as well as any other service provided by a key or important entity pursuant to law or other regulations within the framework of performing activities from Annex I and Annex II of the Act.

(2) Other terms used in this Regulation have the same meaning as the terms used in the Act.

(3) The terms used in this Regulation that have a gender meaning refer equally to the masculine and feminine genders.

Article 5.

The provisions of this Regulation that refer to the competent authorities for the implementation of cyber security requirements also refer to the competent authorities for the implementation of special laws when those provisions regulate issues related to cyber security requirements and their implementation, and which are not regulated by special laws and by-laws adopted on the basis of those laws, in the sense of Article 8 of the Law.

Article 6.

The competent authorities referred to in Annex III to the Act and the single point of contact shall, in accordance with European Union law and relevant national law, safeguard the security and commercial interests of key and important entities and the confidentiality of the information provided in the implementation of their obligations under this Regulation.

PART TWO
CATEGORIZATION OF ENTITIES BY BASIS SPECIAL CRITERIA, CATEGORIZATION PUBLIC SECTOR ENTITIES AND ENTITIES FROM EDUCATION SYSTEM

CHAPTER I.
MEASURES FOR CATEGORIZATION OF SUBJECTS BASED ON SPECIAL CRITERIA

Article 7.

(1) Classification of entities pursuant to Article 11, subparagraph 1. of the Act is implemented for private and public entities from Annex I and Annex II of the Act for which it is determined in the entity categorization process that they are the only service provider in the territory of at least one county, regardless of the number of inhabitants of the cities and municipalities in its composition, due to which the entity is subject to the entity categorization process.

(2) Based on the criteria referred to in paragraph 1 of this Article:

– private and public entities from Annex I of the Act are classified in the category of key entities

– private and public entities from Annex II of the Act are classified in the category of important entities.

Article 8.

(1) The classification of entities pursuant to Article 11, subparagraph 2 of the Act, according to the criterion of the significance of the impact that a disruption in the functioning of the service provided by the entity, or the activity it performs, could have on public safety, shall be carried out for private and public entities from Annex I and Annex II of the Act from which products are directly supplied or services covered by Annex I or Annex II of the Act are ordered for:

– police purposes

– protection of the state border or

– protection and rescue in case of major accidents, disasters and crises.

(2) Based on the criteria referred to in paragraph 1 of this Article:

– private and public entities from Annex I of the Act are classified in the category of key entities

– private and public entities from Annex II of the Act are classified in the category of important entities.

(3) The procedures for categorizing entities referred to in paragraph 1 of this Article shall be carried out upon a reasoned request from a state administration body competent for internal affairs.

Article 9.

(1) Classification of entities pursuant to Article 11, subparagraph 2 of the Act, according to the criterion of the significance of the effect that a disruption in the functioning of the service provided by the entity, or the activity it carries out, would have

performs, could have on public protection, is carried out for private and public entities from Schedule I and Schedule II. of the Act:

– who have been designated by decisions of the competent state administration body as operational forces of the civil protection system of special interest at the state level or are

– by decisions of executive bodies of local and regional self-government units designated as a legal entity of interest for the civil protection system.

(2) Based on the criteria referred to in paragraph 1, subparagraph 1 of this Article, private and public entities from Annex I and Annex II of the Act shall be classified into the category of key entities.

(3) Based on the criteria referred to in paragraph 1, subparagraph 2 of this Article, private and public entities from Annex I and Annex II of the Act shall be classified in the category of significant entities.

(4) The procedures for categorizing entities referred to in paragraph 1 of this Article shall be carried out upon a reasoned request from the state administration body competent for the establishment of the civil protection system.

Article 10.

(1) The classification of entities pursuant to Article 11, subparagraph 2 of the Act, according to the criterion of the significance of the impact that a disruption in the functioning of the service provided by the entity, or the activity performed by the entity, could have on public health, is carried out for healthcare providers from Annex I of the Act that provide one of the following healthcare activities:

– combating infectious diseases

– supply of medicines and medical products for healthcare

– collection and preparation of medical preparations and transplants of human origin or

– emergency medicine.

(2) Health care providers from Annex I of the Act are classified based on the criteria from paragraph 1 of this article into the category of key entities, regardless of whether they provide health services from paragraph 1 of this article at primary, secondary or tertiary level
level.

(3) The procedures for categorizing entities referred to in paragraph 1 of this Article shall be carried out upon a reasoned request from the state administration body responsible for healthcare.

Article 11

(1) Classification of entities pursuant to Article 11, subparagraph 3.
of the Act is implemented for private and public entities from the energy sector, the transport sector, the digital infrastructure sector and providers of managed services and providers of managed security services from the ICT service management (B2B) sector from Annex I of the Act, for which, in the process of categorization of entities, it is determined that the market share of the entity in the provision of services, i.e. the performance of activities for which the entity is the subject of the entity categorization procedure, in the territory of the Republic of Croatia is 25% or more.

(2) The classification of subjects based on Article 11, subparagraph 3 of the Act is also carried out for providers of managed services and providers of managed security services from the ICT service management (B2B) sector from Annex I of the Act that provide management services and managed security services to key and important entities.

(3) Private and public entities from the energy sector, the transport sector, the digital infrastructure sector and managed service providers and managed security service providers from the management sector
ICT services (B2B) from Annex I to the Act are classified in the category of key entities based on the criteria from paragraph 1 of this Article.

(4) Managed service providers and managed security service providers from the ICT service management sector (B2B) from Annex I to the Act are classified in the category of significant entities based on the criteria referred to in paragraph 2 of this Article.

Article 12

(1) Classification of entities pursuant to Article 11, subparagraph 4.
of the Act, according to the criterion of special importance of the entity at the national level, is implemented for private and public entities from Annex I and Annex II of the Act that have been designated as legal entities of special interest for the Republic of Croatia by a decision of the Government of the Republic of Croatia.

(2) Private and public entities from Annex I to the Act shall be classified into the category of key entities based on the criteria from paragraph 1 of this Article.

(3) Private and public entities from Annex II of the Act shall be classified into the category of important entities based on the criteria from paragraph 1 of this Article.

(4) Classification of entities pursuant to Article 11, subparagraph 4.
The Act, according to the criterion of special importance of the subject at the regional and local level, is implemented for:

- private and public entities from the energy sector, the electricity sub-sector, the centralized heating and cooling sub-sector and the gas sub-sector, the water sector for human consumption and the waste water sector from Annex I of the Act

- private and public entities from the postal and courier services sector from Annex II. of the law,

for which, in the process of categorizing entities, it is determined that the market share of the entity in the provision of services, or the performance of the activity for which the entity is subject to the categorizing entity procedure, in the territory of a county, regardless of the number of inhabitants of the cities and municipalities within its composition, is 40% or more.

(5) Private and public entities from the energy sector, electricity sub-sector, district heating and cooling sub-sector and gas sub-sector, water for human consumption sector and wastewater sector from Annex I to the Act shall be classified in the category of key entities based on the criteria referred to in paragraph 4 of this Article.

(6) Private and public entities from the postal and courier services sector from Annex II. of the Act are classified based on the criteria from paragraph 4 of this article into the category of important entities.

Article 13.

Criteria for categorization based on special criteria from Articles 7 to 12 of this Regulation are applied to private and public entities from Annexes I and II. of the Act that are not categorized based on the general criteria for the categorization of entities from Articles 9 and 10 of the Act.

CHAPTER II.
IMPLEMENTATION OF CATEGORIZATION OF PUBLIC SECTOR ENTITIES AND ENTITIES FROM THE EDUCATION SYSTEM

Article 14.

(1) State bodies and legal entities with public powers are classified in the category of key subjects if they meet the following criteria:

- the founder of the entity is the Republic of Croatia, and it is established for the territory of the Republic of Croatia and its activity is performed at the national level, and at the same time it is not categorized in any other sector of high

criticality or other critical sector from Annex I and Annex II.
Law and

– the impact of a significant cyber incident and serious cyber threat on the network and information system of that entity may cause significant:

1. consequences for human life and health or for the environment

2. material and non-material damage to that entity or other legal and natural persons

3. disruptions in the entity's performance of regular activities

4. interdepartmental consequences (influence on other social sectors or economic activities) or

5. negative public influences.

(2) The competent authority for the implementation of cybersecurity requirements, when categorizing public sector entities, shall assess the criteria referred to in paragraph 1, subparagraph 2 of this Article by assessing each of the consequences of the impact of a significant cyber incident and serious cyber threat separately and in relation to other consequences.

Article 15

Units of local and regional (regional) self-government are classified in the category of important entities if they meet at least one of the following criteria:

ÿ perform tasks of regional importance

ÿ represent economic, financial, cultural, health, transport and scientific centers of development of the wider environment

ÿ are authorized to carry out tasks in the field of economic development and planning and development of a network of educational, health, social and cultural institutions or

ÿ they are entrusted with state administration tasks.

Article 16

Subjects from the education system are classified, pursuant to Article 13 of the Act, into the category of important subjects based on an assessment of their special importance for carrying out educational work if they meet at least one of the following criteria:

ÿ provide e-services of national information systems of importance for the education system in the Republic of Croatia

ÿ they represent a higher education institution that conducts applied scientific research for the purpose of innovation and technology development, regardless of the founder of the institution

ÿ represent a higher education institution that provides information services systems important for the education system in the Republic of Croatia or

ÿ represent a public institution that conducts external evaluation in the education system of the Republic of Croatia and examinations based on national standards.

PART THREE

LISTS OF KEY AND IMPORTANT ENTITIES AND SPECIAL REGISTER OF ENTITIES

CHAPTER I.

OBLIGATIONS OF THE ENTITIES IN ANNEX I AND ANNEX II LAW

Article 17.

(1) Those obliged to submit data for the categorization of subjects and those obliged to submit data for maintaining a special register of subjects They are required to appoint a contact person responsible for data submission.

(2) The contact person responsible for submitting data must be:

ÿ an appointed person from among the members of the entity's management body

ÿ an appointed person from among state officials in state administration bodies and other state bodies or

ÿ appointed executive body of a unit of local and regional self-government.

Article 18

(1) The contact person responsible for the submission of data is responsible for the timely submission of accurate and complete data and notification of changes to data in accordance with Articles 20 and 23 of the Act and the provisions of this Regulation.

(2) The contact person responsible for the delivery of data is obliged to appoint at least two persons authorized to operationalize the delivery of data and notification of data changes from Articles 20 and 23 of the Act.

Article 19

(1) Persons obliged to submit data for the categorization of entities and persons obliged to submit data for the maintenance of a special register of entities shall, without delay and no later than eight days from the date of receipt of the request referred to in Article 20, paragraph 1 and Article 23, paragraph 2 of the Act, submit data on the designated contact person responsible for the submission of data and the persons authorised to operationalise the submission, as follows:

ÿ name and surname of the appointed persons

ÿ information about their workplace or duties in the entity

ÿ the email address of the contact person responsible for submitting the data and

ÿ e-mail addresses that persons authorized to operationalize delivery will use for the purposes of delivering data and notifying about changes to data.

(2) In the event of a change in the persons referred to in paragraph 1 of this Article or in individual data submitted in accordance with paragraph 1 of this Article, those obliged to submit data for the categorization of entities and those obliged to submit data for the maintenance of a special register of entities shall be obliged to notify the competent body for the implementation of the categorization of entities or the competent body for the maintenance of a special register of entities of the change, without delay, and no later than 15 days from the date of appointment of the new person or change in individual data submitted in accordance with paragraph 1 of this Article.

(3) The notifications referred to in paragraphs 1 and 2 of this Article shall be submitted to the competent authority responsible for implementing the categorization of entities, or to the competent authority responsible for maintaining a special register of entities, in accordance with the instructions referred to in Article 22 of this Regulation.

Article 20

Those obliged to submit data for the categorization of entities are obliged to submit data and notifications on changes in data referred to in Article 20 of the Act to the competent authority for the implementation of the categorization of entities as follows:

ÿ "name of the entity" is the name or title under which the entity operates or carries out its activities in the Republic of Croatia, with an indication of the abbreviated name or title, if the entity uses it in legal transactions, and the personal identification number of the entity (hereinafter: OIB)

ÿ "address" means the address of the entity's registered office, and the address of the contact person responsible for submitting data, if different from the address of the entity's registered office

- "updated contact information, including e-mail addresses" website address of the subject, name and surname of the contact person responsible for the delivery of data and persons authorized to operationalize the delivery, telephone numbers, mobile phone numbers and e-mail addresses of the contact person responsible for the delivery of data and persons authorized to operationalize the delivery

ÿ "IP address ranges" IP address ranges used by the entity in the Republic of Croatia

- »relevant sector, sub-sector and type of entity from Annex I and Annex II. of the Act" names of sectors, sub-sectors and types of entities, according to the names from Annex I of this Regulation

ÿ "list of Member States in which the entity provides services covered by the scope of the Act" means a list of Member States of the European Union (hereinafter referred to as: Member States) in which the entity provides services or performs activities from Annex I or Annex II of the Act and the legal form of the provision or performance of these activities in other Member States and

ÿ "other data on the provision of its services or the performance of its activities relevant for the implementation of the categorization of the entity or the determination of jurisdiction over the entity" data on the size of the entity and other data requested from the entity by the competent body for the implementation of the categorization of entities, for the purpose of implementing the categorization of the entity or the determination of jurisdiction over the entity.

Article 21

Those obliged to submit data for maintaining a special register of entities are obliged to submit data and notifications about changes in data referred to in Article 23 of the Act to the competent authority for maintaining a special register of entities as follows:

ÿ "name of the entity" is the name or title under which the entity operates or carries out its activities in the Republic of Croatia, with an indication of the abbreviated name or title, if the entity uses it in legal transactions, and the OIB (Tax Identification Number)

ÿ "address of the principal place of business of the entity" means the address of the principal place of business of the entity within the meaning of Article 14, paragraphs 3 and 4 of the Act

ÿ "list of services referred to in Article 22 of the Act" a list of services referred to in Article 22 of the Act provided by the entity in the Republic of Croatia

ÿ "addresses of business units in the Republic of Croatia" addresses of all business units of the entity located in the Republic of Croatia

ÿ "IP address ranges" IP address ranges used by the entity in the Republic of Croatia

ÿ "list of other Member States in which the entity operates" means a list of other Member States in which the entity provides the services referred to in Article 22. Law

- "addresses of other business units" addresses of the entity's business units where the entity provides services from Article 22 of the Act located in other member states and

ÿ "updated contact details, including e-mail addresses and telephone numbers of the entity" the address of the entity's website, the name and surname of the contact person responsible for submitting the data, the telephone number, mobile phone number and e-mail address of the contact person responsible for submitting the data, if the entity has its main place of business in the Republic of Croatia within the meaning of Article 14, paragraphs 3 and 4 of the Act or

- "name and address of the representative, updated contact information, including e-mail addresses and telephone numbers of the representative" the name of the the name, address, telephone number, mobile phone number and e-mail address of a natural or legal person established in the Republic of Croatia or another Member State, who has been expressly appointed by the person obliged to provide data for the purpose of maintaining a special register of entities not established in the European Union to act on his behalf and who the competent authority may address instead of the entity itself in relation to the obligations of that entity under this Regulation.

Article 22

(1) The data referred to in Articles 20 and 21 of this Regulation and notifications of their changes shall be submitted in electronic form, in accordance with the instructions published on their websites by the competent authorities responsible for implementing the categorization of entities and the competent authority responsible for maintaining the special register of entities.

(2) The competent authorities responsible for implementing the categorization of entities and the competent authority responsible for maintaining a special register of entities are obliged to define in the instructions referred to in paragraph 1 of this Article the method of delivery in exceptional cases when delivery in electronic form is not possible for justified reasons.

(3) The competent authority for maintaining a special register of entities shall, in the instructions referred to in paragraph 1 of this Article, define the method of compiling and submitting data and notifications of data changes in cases where the same entities are obliged to submit data and notifications of data changes based on the obligations arising for those entities as data providers for maintaining a special register of entities and data providers for the categorization of entities.

Article 23

(1) The instructions from Article 22 of this Regulation also contain instructions for the voluntary delivery of data for the purpose of implementing the subject categorization procedure.

(2) Submission of data on the subject in accordance with the instructions for voluntary submission of data referred to in paragraph 1 of this Article shall be considered equivalent to submission of data at the request of the competent authority for the implementation of cybersecurity requirements referred to in Article 20, paragraph 1 of the Act.

(3) The submission of data on the entity in accordance with paragraphs 1 and 2 of this Article does not affect the obligation to inform the entity about the categorization carried out in accordance with Article 19 of the Act.

(4) The submission of data on an entity in accordance with paragraphs 1 and 2 of this Article shall not affect the obligations of the entity referred to in Articles 17 to 19 of this Regulation.

Article 24.

(1) If data or notifications of changes in data have not been submitted in accordance with Articles 19 to 23 of this Regulation, the competent authority for the implementation of the categorization of entities and the competent authority for maintaining a special register of entities shall notify the entity thereof and set a deadline within which the entity is obliged to eliminate the deficiencies and submit the data, i.e. the change, amendment or correction of the data, with a warning of the legal consequences in accordance with the Law if it fails to do so within the set deadline.

(2) The notification referred to in paragraph 1 of this Article shall be delivered to the email address of the contact person responsible for submitting data, or to the email address of the representative of the person obliged to submit data for maintaining a special register of entities not established in the European Union.

CHAPTER II.
COLLECTING DATA FROM OTHER SOURCES

Article 25

(1) For the purpose of implementing the obligations from Article 21, subparagraph 1 of the Act, state administration bodies, other state bodies, local units and

social (regional) self-governments, legal entities with public powers and public entities are obliged to keep a list of entities from Annex I and Annex II. of the Act, for which they collect data within their scope, or maintain registers, records and data collections.

(2) The list of entities referred to in paragraph 1 of this Article shall contain the following information:

– sectors, sub-sectors and types of entities from Annex I and Annex II. of the Act for which they collect data, i.e. keep registers, records and data collections, according to the names from Annex I of this Regulation

– for each sector, sub-sector and type of entity referred to in subparagraph 1 of this paragraph, the names of the entities or the names or names under which the entities operate or perform the activities referred to in Annex I and Annex II of the Act in the Republic of Croatia, with an indication of the abbreviated name or name, if the entity uses it in legal transactions

- the legal basis on the basis of which they collect data, i.e. keep registers, records and collections of data on entities from sub-paragraph 2 of this paragraph

- an indication of whether they keep registers, records and collections of data related to the size of entities in the sense of Article 15 of the Act and what data they collect and

– information on whether they keep registers, records and data collections for the entities referred to in subparagraph 2 of this paragraph in electronic form, with a statement on the possibilities of accessing data in these registers, records and data collections electronically.

(3) The lists of entities referred to in paragraph 1 of this Article shall be submitted in accordance with the instructions published on their websites by the competent authorities responsible for implementing the categorization of entities.

(4) The lists of entities referred to in paragraph 1 of this Article shall be submitted to the competent authorities for the implementation of the categorization of entities once a year, no later than 1 March of the current year for the previous year.

(5) By way of exception to paragraph 4 of this Article, if there have been no changes in relation to the previously submitted list of entities, state administration bodies, other state bodies, local and regional self-government units, legal entities with public authority and public entities shall notify the competent body responsible for implementing the categorization of entities thereof, without the obligation to submit a new list of entities.

(6) By way of exception to paragraphs 1 and 4 of this Article, state administration bodies, other state bodies, local and regional self-government units, legal entities with public authority and public entities are not obliged to maintain and regularly submit lists of entities referred to in paragraph 1 of this Article, if they have provided the competent bodies responsible for implementing the categorization of entities with electronic access to the relevant data on entities in registers, records and databases.

Article 26

Article 25 of this Regulation does not apply to:

– banking sector

– financial market infrastructure sector and

– sub-sector of air transport.

CHAPTER III.

METHOD OF MAINTAINING AND CONTENT OF THE LIST OF KEY AND IMPORTANT ENTITIES

Article 27.

(1) Lists of key and important entities shall be kept in electronic form.

(2) In the Lists of key and important subjects, the data prescribed by this Regulation and all changes to these data are entered, in such a way that the originally entered data and subsequently entered changes to these data are visible.

Article 28.

(1) Lists of key and important subjects are kept by sectors, sub-sectors and types of subjects from Annex I and Annex II. of the Act, according to the names from Annex I of this Regulation.

(2) Lists of key and important entities contain general information about to the subject and data on the carried out categorization of the subject.

(3) The following data shall be entered in the Lists of Key and Important Entities under "general data on the entity":

– name of the entity

– Subject's OIB

– subject address

– telephone number, mobile phone number and email address of the contact person responsible for submitting the data

– IP address ranges used by the entity in the Republic of Croatia

– list of Member States in which the entity provides services or performs activities from Schedule I or Schedule II. of the Law

– date of entry of the entity into the List of Key and Important Entities.

(4) In the Lists of key and important subjects under "data on implementation The following data is entered in the "Subject Categorization" field:

– information on the category of the entity, i.e. an indication of whether the entity is classified as a key and/or important entity

- information on the basis of which provision of the Act the categorization of the subject was carried out

- the name of the sector, sub-sector and type of entity into which the entity is classified, according to the names from Annex I of this Regulation

– date of subject categorization

– the mandatory level of risk management measures established for the entity Bernetic security risks from Article 38 of this Regulation

– date of notification of the categorization of the entity referred to in Article 19, paragraphs 1 and 2 of the Act, when applicable

– a note on whether a protocol on the actions of the competent authorities referred to in Article 59, paragraph 3 of the Act has been drawn up for the entity, when applicable

– date of the verification of the List referred to in Article 17, paragraph 2 of the Act.

(5) General information about the entity shall be entered in the List of Key and Important Entities based on the information submitted in accordance with Articles 19, 20, 22 and 23 of this Regulation.

(6) Data on the implemented categorization of the entity and the mandatory level of cyber security risk management measures shall be entered based on data determined in the entity categorization process or conducted checks of the List of Key and Important Entities referred to in Article 17, paragraph 2 of the Act.

Article 29

(1) The competent authorities responsible for implementing the categorization of entities are obliged to enter the entity in the List of Key and Important Entities no later than eight days from the date of the categorization of the entity.

(2) The competent authorities responsible for implementing the categorization of entities are obliged to enter the change in the entity category and other related data in the List of Key and Important Entities no later than eight days from the date of delivery of the notification referred to in Article 19, paragraph 2 of the Act.

(3) The competent authorities responsible for implementing the categorization of entities are obliged to enter changes to general data about the entity within eight days.

from the date of receipt of notification of changes in the data referred to in Articles 19 and 20 of this Regulation.

Article 30

(1) Competent authorities for the implementation of the categorization of entities are obliged to keep entities that, after updating the List of key and important entities, are no longer considered either key entities or important entities in the List of key and important entities with the indication "inactive".

(2) Competent authorities for the implementation of the categorization of entities are obliged to check the List of key and important entities from Article 17, paragraph 2 of the Act to include the entities from paragraph 1 of this Article, unless the entity was found to have ceased operations in the previous verification procedure.

Article 31

(1) For the purpose of implementing the obligations referred to in Article 18, paragraph 2 of the Act, the competent authorities responsible for implementing the categorization of entities are obliged to submit data on the implemented categorization of entities to the single point of contact in accordance with the guidelines of the single point of contact on the content, method of submission and deadlines for submission of notifications on the implemented categorization of entities.

(2) For the purpose of implementing Article 43 of the Act, the competent authorities for implementing the categorization of entities are obliged to submit the Lists of key and important entities, including all subsequent updates to the List, in a timely manner and in an appropriate format to the Croatian Academic and Research Network – CARNET (hereinafter: CARNET).

CHAPTER IV.
METHOD OF KEEPING AND CONTENT OF THE SPECIAL REGISTER OF SUBJECTS

Article 32

(1) A special register of entities shall be kept in electronic form.

(2) The data prescribed by this Regulation and all changes to such data shall be entered into the Special Register of Entities, in such a way that the originally entered data and any subsequently entered changes to such data are visible.

Article 33.

(1) The following data shall be kept in the Special Register of Entities:

– name of the entity

– Subject's OIB

– list of services referred to in Article 22 of the Act provided by the entity in the Republic of Croatia

– address of the entity's principal place of business

– addresses of business units of the entity in the Republic of Croatia

– IP address ranges used by the entity in the Republic of Croatia

– list of other Member States in which the entity provides services referred to in Article 22 of the Act

– addresses of business units of the entity in which the entity provides services referred to in Article 22 of the Act, which are located in other member states

– telephone number, mobile phone number and email address of the contact person responsible for submitting the data or the entity's representative, if the entity does not have a business establishment in the European Union

– date of entry of the entity into the Special Register of Entities.

(2) Data on the entity shall be entered into the Special Register of Entities on the basis of data submitted in accordance with Articles 19, 21 and 22 of this Regulation.

Article 34.

For the purpose of implementing the obligations referred to in Article 23, paragraph 4 of the Act, the competent authority for maintaining a special register of entities is obliged to submit data on entities referred to in Article 22 of the Act, via a single point of contact, to the European Cybersecurity Agency (hereinafter: ENISA) within the deadlines and in the manner defined by its guidelines.

PART FOUR
CYBERNETIC SECURITY MANAGEMENT RISKS

CHAPTER I.
NATIONAL ASSESSMENT OF CYBERNETIC SECURITY RISKS

Article 35

(1) As part of the entity categorization process, a national cybersecurity risk assessment (hereinafter: national risk assessment) shall be conducted for each entity categorized as a critical or important entity.

(2) The aim of conducting a national risk assessment is to define the level of cybersecurity risk management measures that each individual entity categorized as a critical or important entity is required to implement.

Article 36

The national risk assessment is carried out based on data on:

– the size of the subject and

- the subject's belonging to a certain sector from Annex I and Annex II. of the law,

as well as based on monitoring the state of cybersecurity globally at the national and regional levels and conducting related assessments:

- a selection of typical types of cyberattacks, which are taken as relevant for this assessment, such as: business disruption or sabotage, data theft or espionage, cybercrime, vandalism of content and data availability on the Internet, political influence and disinformation

– whether a particular type of typical cyberattack is generally possible in a sector or is it assessed as targeted for a particular sector

– levels of severity of disruptions in the functioning of services or the performance of activities that selected types of typical cyberattacks can cause in a particular sector, according to available data

– selecting typical types of cyber attackers that are considered relevant for this assessment, such as: state-sponsored APT groups, terrorists, cybercriminal groups, hacktivist groups, competitive business attackers, along with an assessment of the typical level of cyber skills of selected types of attackers

– the probability of the occurrence of a particular type of cyberattack, caused by a particular type of cyberattacker for each individual sector and for all selected typical types of cyberattacks, as well as for all selected types of cyberattackers.

Article 37.

(1) The necessary elaboration of data and assessments referred to in Article 36, for the purpose of implementing a national risk assessment for entities in the sectors referred to in Annex I and Annex II of the Act, shall be carried out by the central state authority for

cybersecurity, in cooperation with other competent authorities for the implementation of cybersecurity requirements.

(2) The national risk assessment for each individual entity, which is categorized within the area of jurisdiction of an individual competent authority for the implementation of cybersecurity requirements, based on the data and assessments referred to in paragraph 1 of this Article, shall be carried out by the competent authority for the implementation of cybersecurity requirements.

(3) The national risk assessment referred to in paragraph 2 of this Article shall be carried out as part of the first entity categorization procedure, after each update of the list of key and important entities pursuant to Article 17, paragraph 2 of the Act, and during each categorization of an entity carried out by the competent authority for the implementation of cybersecurity requirements.

Article 38.

(1) The result of the national risk assessment is the determination of a low, medium or high level of cybersecurity risks for each individual entity referred to in Article 37, paragraph 2 of this Regulation.

(2) Depending on the determined level of cybersecurity risks, each entity categorized as a critical or important entity is required to implement one of three levels of cybersecurity risk management measures, as follows:

- for a low level of estimated cyber security risks, by categorization, the subject is obliged to implement the basic level of cyber security risk management measures from Article 42, paragraph 1 and Annex II. of this Regulation

- for the medium level of the estimated cyber security risks, by categorization, the subject undertakes to implement the medium level of cyber security risk management measures from Article 42, paragraph 2 and Annex II. of this Regulation

- for a high level of estimated cyber security risks, by categorization, the entity undertakes to implement an advanced level of cyber security risk management measures from Article 42, paragraph 3 and Annex II. of this Regulation.

Article 39

(1) If the entity provides services or performs activities that belong to several different sectors from Annex I and Annex II. of the Act, the national risk assessment is carried out for the subject's main activity.

(2) If the subject's main activity cannot be unequivocally determined, a national risk assessment is carried out for all services and activities due to the provision or performance of which the subject is categorized as a key or important subject, and the highest level of cyber security risks thus determined is taken as the final national risk assessment of the subject.

Article 40

(1) The national risk assessment and the determination of the binding level of cybersecurity risk management measures for key and important entities referred to in Article 38 of this Regulation shall be carried out in accordance with the guidelines for the implementation of the national cybersecurity risk assessment, which are prepared on the basis of data and assessments referred to in Article 36 of this Regulation and of which an integral part is the corresponding calculator for calculating the level of cybersecurity risks.

(2) The guidelines for the implementation of the national risk assessment referred to in paragraph 1 of this Article, which describe the procedure for calculating the risk based on the data and estimates referred to in Article 36 of this Regulation, as well as the use of the associated calculator, shall be issued by the central state authority for cybersecurity.

(3) The central state authority for cybersecurity shall publish the guidelines referred to in paragraph 2 of this Article on its website.

CHAPTER II.
CYBER SECURITY MANAGEMENT MEASURES RISKS

Article 41

The list of cybersecurity risk management measures is set out in Annex II to this Regulation for all three levels of cybersecurity risk management measures referred to in Article 38 of this Regulation.

Article 42

(1) The basic level of cybersecurity risk management measures referred to in Article 38, paragraph 2, subparagraph 1 of this Regulation represents a general set of cybersecurity practice measures that can be achieved with readily available technologies and well-known and documented best cybersecurity practices, appropriate in the case of entities whose activities belong to sectors that are not typically targeted cyberattacks carried out by attackers with a higher level of cyber skills, and the aim of applying the basic level is to protect the entity from the majority of globally present cyberattacks, i.e. from cyberattacks carried out by cyberattackers with average cyber skills.

(2) The medium level of cybersecurity risk management measures referred to in Article 38, paragraph 2, subparagraph 2 of this Regulation represents an supplemented set of cybersecurity practice measures that builds on the basic level of cybersecurity risk management measures, and the aim of applying the medium level is to further reduce the risks of targeted cyber attacks carried out by cyber attackers with average cyber skills.

(3) The advanced level of cybersecurity risk management measures referred to in Article 38, paragraph 2, subparagraph 3 of this Regulation represents an supplemented set of cybersecurity practice measures that builds on the intermediate level of cybersecurity risk management measures, and the aim of applying the advanced level is to reduce the risk of advanced cyber attacks carried out by cyber attackers with advanced skills and resources.

Article 43

List of cyber security risk management measures from Annex II. of this Regulation, for each measure contains:

– name of the measure

– objective of the measure

- elaboration of the measure into subsets of cyber security risk management measures

– applicability of the measure in the context of IT and OT systems and

- tabular representation of the distribution of subsets of measures from sub-paragraph 3. of this paragraph by the levels of measures referred to in Article 38 of this Regulation.

Article 44.

(1) Subsets of cybersecurity risk management measures whose implementation is mandatory within a certain level of measures referred to in Article 38 of this Regulation are marked with the symbol "A" in the table referred to in Article 43, subparagraph 5 of this Regulation.

(2) Subsets of cyber security risk management measures whose implementation within a certain level of measures referred to in Article 38 of this Regulation is mandatory under the conditions described in the elaboration of the measure referred to in Article 43, subparagraph 4 of this Regulation under "CONDITION:", are marked in the table referred to in Article 43, subparagraph 5 of this Regulation with the symbol "B".

(3) Subsets of cybersecurity risk management measures whose implementation falls within a certain level of measures referred to in Article

38 of this Regulation, are marked with the symbol "C" in the table from Article 43, subparagraph 5 of this Regulation.

Article 45

(1) Subsets of cybersecurity risk management measures marked with the symbol "C" in the table referred to in Article 43, subparagraph 5 of this Regulation are recommended for implementation depending on the results of the risk assessment carried out by the entity within the framework of the implementation of the measure entitled "Risk Management" referred to in point 3 of Annex II of this Regulation.

(2) The implementation of the subsets of cyber security risk management measures that are marked with the symbol "C" in the table from Article 43, sub-paragraph 5 of this Regulation is additionally evaluated through the cyber security self-assessment and cyber security audit procedure.

(3) For the purposes of implementing the risk assessment referred to in paragraph 1 of this Article, the central state authority for cybersecurity shall adopt guidelines for the assessment, processing, monitoring and updating of risks for network and information systems, which may be used within the framework of the implementation of the measure entitled "Risk Management" referred to in point 3 of Annex II to this Regulation.

(4) The central state authority for cybersecurity shall publish the guidelines referred to in paragraph 3 of this Article on its website.

Article 46

(1) Services provided, that is, activities performed by private and public entities from the digital infrastructure sector from Annex I.
of the Act, are based on network and information systems, and this Regulation establishes a special, expanded set of physical security measures for these types of entities as part of the cyber security risk management measures that these entities are required to implement.

(2) The expanded set of physical security measures referred to in paragraph 1 of this article is determined by Annex III. of this Regulation.

Article 47

(1) For the purpose of implementing voluntary cyber protection mechanisms referred to in Article 50 of the Act, entities that are not categorized as critical and important entities shall implement at least a basic level of cybersecurity risk management measures.

(2) In cases referred to in Article 60 of the Act, the competent authorities for the implementation of cybersecurity requirements are obliged to implement an advanced level of cybersecurity risk management measures.

Article 48.

All implemented cyber security risk management measures, key and important entities and entities from Article 47 of this Regulation must be updated:

– at planned time periods, and at least once
annually as part of the entity's regular annual risk assessment

– when a significant incident occurs

– when they implement significant changes within the network and information system

– within the framework of major business and organizational changes, mergers or changes in the ownership structure of the entity that may have an impact on the management of the entity

– when the entity's non-compliance is determined in the cyber security audit or cyber security self-assessment process or

– when corrective measures are imposed on the subject in the expert procedure oversight over the implementation of cybersecurity requirements.

Article 49

(1) In order to facilitate the implementation of cyber security risk management measures, the central state authority for cyber security shall to ensure safety, he prepares a correlational overview of the measures from Annex II. of this Regulation, as well as all subsets of these measures, to the most important European and international norms and best practices from open sources (mapping of measures).

(2) The central state authority for cybersecurity shall publish the correlation overview referred to in paragraph 1 of this Article on its website.

Article 50

In order to raise the level of cybersecurity of entities that are not categorized as key or important entities and do not implement voluntary cybersecurity protection mechanisms referred to in Article 50 of the Act, entities that are just starting to introduce cybersecurity risk management measures or represent micro or small businesses with limited resources and knowledge in cybersecurity risk management issues, the central state cybersecurity authority prepares and publishes on its website recommendations for the implementation of good cybersecurity practices.

CHAPTER III.
CYBER SECURITY SELF-ASSESSMENT

Article 51

(1) The cybersecurity self-assessment determines the degree of compliance of the established cybersecurity risk management measures with the cybersecurity risk management measures from Annex II to this Regulation established for the level of cybersecurity risk management measures from Article 38 of this Regulation that the entity is required to implement, as well as the trend of increasing the level of cybersecurity maturity of the entity.

(2) Self-assessment of cyber security is carried out by important entities and subjects from Article 47 of this Regulation at least once every two years.

(3) Self-assessment of cyber security can be carried out by key entities as a preparation for the implementation of a cyber security audit or expert supervision over the implementation of cyber security requirements from Article 75, paragraph 1 of the Act.

Article 52

(1) The degree of compliance of the established measures is based on an assessment of the degree of compliance of the documented and implemented cybersecurity risk management measures in the entity.

(2) The assessment of the level of compliance of documented cybersecurity risk management measures determines whether there are documented security policies on the implementation of measures and to what extent they comply with the requirements set out for cybersecurity risk management measures in Annex II to this Regulation, for the level of cybersecurity risk management measures referred to in Article 38 of this Regulation that the entity is required to implement.

(3) The assessment of the level of compliance of implemented cybersecurity risk management measures determines the extent to which the established cybersecurity risk management measures are compliant with the requirements set out for cybersecurity risk management measures in Annex II to this Regulation, for the level of cybersecurity risk management measures referred to in Article 38 of this Regulation that the entity is required to implement.

Article 53

(1) The degree of compliance of established measures from Article 52, paragraphs 2 and 3 of this Regulation is determined based on the scoring of subsets

a cybersecurity risk management measure that the entity implements as mandatory in accordance with Article 44, paragraphs 1 and 2 of this Regulation.

(2) For the purpose of implementing the scoring referred to in the previous paragraph of this Article, for each level of cybersecurity risk management measures referred to in Article 42 of this Regulation, the number of points required to confirm the entity's compliance with the level of cybersecurity risk management measures determined to be binding for the entity in accordance with Article 38 of this Regulation shall be determined.

Article 54.

(1) The trend of increasing the level of cybersecurity maturity is determined by additional scoring of subsets of cybersecurity risk management measures implemented by the entity based on measure 3. "Risk management" from Annex II of this Regulation, in terms of increasing the level of implementation of individual mandatory measures in accordance with Article 44, paragraphs 1 and 2 of this Regulation, as well as in terms of implementing voluntary measures in accordance with Article 44, paragraph 3 of this Regulation.

(2) For the purpose of implementing the scoring referred to in the previous paragraph, for each level of cybersecurity risk management measures referred to in Article 42 of this Regulation, the number of points required to determine the trend of increasing the level of cybersecurity maturity of the entity shall be determined.

Article 55

(1) If the results of the scoring of the degree of compliance of measures in accordance with Article 53 of this Regulation show that the cybersecurity risk management measures have been established in accordance with the level of cybersecurity risk management measures determined to be binding for the entity in accordance with Article 38 of this Regulation, the entity shall draw up a declaration of compliance referred to in paragraph 3 of this Article.

(2) If the results of the scoring of the degree of compliance of measures in accordance with Article 53 of this Regulation show that cybersecurity risk management measures have not been established in accordance with the level of cybersecurity risk management measures determined to be binding for the entity in accordance with Article 38 of this Regulation, the entity shall establish a plan for further action, which shall include a plan for a timely re-assessment of cybersecurity self-assessment and correction of identified deficiencies.

(3) The declaration of conformity referred to in Article 35, paragraph 3 of the Act shall contain the following information:

– name and address of the entity

– name of the sector, subsector and type of entity, according to the names from Annex I of this Regulation, for key and important subjects, ie

- the name of the sector and the main business activity for entities from Article 47, paragraph 1 of this Regulation

– the identified level of cybersecurity risks for the entity, where applicable

– the level of cybersecurity risk management measures that has been determined to be binding on the entity in accordance with Article 38 of this Regulation

– the results of the scoring of the degree of compliance of cybersecurity risk management measures with the level of cybersecurity risk management measures determined to be binding for the entity in accordance with Article 38 of this Regulation

– results of scoring the trend of raising the level of maturity of the entity's cyber security

– list of documentation generated during the cyber security self-assessment process

– name, surname and signature of the person who carried out the self-cybersecurity assessments

– a statement by the person responsible for managing cybersecurity risk management measures that the results of the conducted cybersecurity self-assessment for the entity show that cybersecurity risk management measures have been established in accordance with the cybersecurity risk management measures prescribed by the Act and this Regulation

– name, surname and signature of the person responsible for managing cyber security risk management measures.

(4) The entity shall draw up the declaration of conformity referred to in Article 35, paragraph 3 of the Act on the form set out in Annex IV to this Regulation.

(5) The entity is obliged to keep the declaration of compliance referred to in Article 35, paragraph 3 of the Act and other documentation created in the cybersecurity self-assessment process for ten years from the date of drawing up such a declaration.

Article 56

To conduct a cybersecurity self-assessment, the entity is required to designate its employees or external collaborators who possess at least:

– relevant knowledge from the implementation of international norms in the field of information or cyber security

- certificate of completed external or internal training for an internal auditor according to one of the relevant international norms in the field of information or cyber security

– one year of work experience in conducting similar types of internal audits in the field of network and information systems, or cybersecurity.

Article 57

(1) The central state body for performing tasks in the technical areas of information security shall issue guidelines for the implementation of cybersecurity self-assessments, an integral part of which is a calculator for scoring and calculating the degree of compliance of the established cybersecurity risk management measures and the trend of increasing the level of cybersecurity maturity of the entity.

(2) The central state body responsible for performing tasks in the technical areas of information security shall publish the guidelines referred to in paragraph 1 of this Article on its website.

PART FIVE
CYBER NOTIFICATION RULES THREATS AND INCIDENTS FOR KEY AND IMPORTANT ENTITIES

CHAPTER I.
NOTICE OF SIGNIFICANT INCIDENTS

Article 58

A significant incident is any incident that meets at least one of the criteria for determining significant incidents from Articles 59 to 62 of this Regulation, taking into account the criterion thresholds, when they are prescribed.

SECTION 1
CRITERIA FOR DETERMINING SIGNIFICANT INCIDENTS

Article 59

(1) Incidents that cause or may cause serious disruptions in the functioning of services are incidents:

– which negatively affect the availability of the service or impair the quality of the service or

– have or may have a negative impact on the authenticity, integrity or confidentiality of stored, transmitted or processed data or services.

(2) An incident is considered to negatively impact service availability or impair service quality if at least one of the following criteria thresholds is met:

– at least 20% of service recipients were unable to access the service lasting at least one hour

– at least 1% of service recipients were unable to access the service for at least eight hours, provided that 1% of service recipients constitute at least 100 service recipients

– access to the service was not possible for a period of one hour or more, and the entity is not able to determine how many recipients of the service were unable to access the service during the period of time in which the service was unavailable

– at least 30% of service recipients were occasionally unable to access the service or were unable to use the service functionally due to a reduced level of service quality, if the occasional interruptions in access to the service, or the inability to use the service functionally, lasted a total of at least one hour during a four-hour period

– access to the service at a hospital, airport, airline, bank facility with data centers, police system facility, active water pumping station and control center, electronic communications operator facility, security intelligence system body facility, professional fire department facility or entity determined as critical entities under the law regulating the area of critical infrastructure was not possible for at least one hour

– access to the air traffic control service was not possible, regardless of the duration of the interruption of access to the service and the number of recipients to whom the service was not available

– access to the service used for the needs of the Ministry of Defense and the Armed Forces of the Republic of Croatia, civilian holders of defense planning, or for the needs of legal entities of particular importance for defense was not possible for at least one hour

– access to the 112 Center and other emergency services was not possible, regardless of the duration of the interruption of access to the service and the number of recipients to whom the service was not available

– access to the service in the area of at least one county or one large city or the city that is the seat of a county was not possible for at least one hour.

(3) An incident is considered to have or may have a negative impact on the authenticity, integrity or confidentiality of stored, transmitted or processed data or services if at least one of the following criteria thresholds is met:

– critical parts of the entity's network and information system or critical data have been accessed by an unauthorized person or the prerequisites for access by an unauthorized person have been met

– the entity's critical network and information systems have been configured by an unauthorized person or prerequisites have been acquired that enable the configuration of a critical network and information system by an unauthorized person

– due to the incident, circumstances have arisen that prevent the authorized person from configuring the critical network and information system

– the configuration of the subject's critical network and information system has been unauthorized changed, supplemented or has become unreliable for other reasons or critical data has been removed, changed, supplemented or has become unreliable for other reasons

– the entity's critical network and information systems and/or other network and information systems of the entity that may affect the entity's critical network and information systems perform tasks that deviate from the established procedures for performing business activities on the system and/or the established control framework within which these systems normally operate, and in particular if they perform tasks that these systems are not intended to perform or do not perform the basic tasks that these systems are intended to perform.

(4) For the purposes of paragraph 3 of this Article, all systems and data are considered critical if the entity has not conducted a classification of the criticality of network and information systems, has not identified critical data or cannot identify critical network and information systems or critical data that have been negatively affected by the incident.

Article 60

(1) An incident is considered to cause or may cause financial losses for the entity if at least one of the following criteria thresholds is met:

– if the loss of income or costs caused by the incident or the sum of these two factors amounts to one hundred thousand euros or at least 5% of the entity's total annual business revenue, whichever is lower

– if access to the service was not possible for at least one hour for recipients of services from which the entity generated revenue in the amount of one hundred thousand euros or at least 5% of the entity's total annual business revenue in the previous year, whichever is lower

– if the incident caused reputational damage to the subject.

(2) The total annual business income of an entity in the sense of paragraph 1 of this Article shall be considered the total annual business income of the entity according to the financial statements for the previous year, regardless of whether the entity provides other services or performs other activities that are not included in Annex I and Annex II. of the Law.

(3) Income within the meaning of paragraph 1 of this Article shall be considered all income of an entity on an annual basis, regardless of whether it is generated or planned to be generated through the entity's regular operations or through activities that fall outside the scope of the entity's regular operations.

(4) Costs within the meaning of paragraph 1 of this Article shall be considered to be all costs incurred by the entity due to taking actions and activities to stop the incident, respond to the incident or recover from the incident, including all actions and activities taken to establish the regular scope of the entity's business. Costs shall not include contractual penalties or other types of compensation that the entity is obliged to pay due to a breach of contractual relations caused by the incident, regardless of whether they concern natural or legal persons, employees of the entity or its external collaborators.

(5) The incident is considered to have caused damage to the subject's reputation in the sense of paragraph 1, subparagraph 3 of this Article, if one of the following criterion thresholds is met:

– the incident was reported by a public media service provider

– the incident resulted in complaints, lawsuits or other legal remedies being filed against the entity by at least 1% of recipients of its services.

Article 61

(1) The incident is considered to have affected or could have affected other natural and legal persons by causing significant material or

non-material damage, if one of the following occurred as a result of the incident:

– death or bodily injury that required hospitalization or therapeutic procedures

– complete destruction or significant damage to material property
other natural or legal persons

– suspension or significant reduction of business operations of other natural or legal persons

– loss or compromise of personal or sensitive data
other natural or legal persons.

(2) Other natural and legal persons within the meaning of paragraph 1 of this Article are considered to be recipients of services of a key and important entity, as well as any other natural and legal person who has suffered material or non-material damage from paragraph 1 of this Article due to a significant incident.

Article 62

Incidents that individually do not meet the criteria for a significant incident from Articles 59 to 61 of this Regulation will be considered a significant incident if:

– occurred at least twice within a six-month period

– have the same underlying cause

- together they meet at least one criterion for a significant incident from Articles 59 to 61 of this Regulation.

Article 63

Interruptions in the provision of service or disruption of service quality due to planned regular maintenance of the network and information systems of key and important entities are not considered a significant incident within the meaning of Articles 59 to 62 of this Regulation.

SECTION 2
NOTIFICATIONS OF SIGNIFICANT INCIDENTS

Article 64.

Key and important entities are required to notify the competent CSIRT of any significant incident.

Article 65

Key and important entities are required to submit the following types of notifications about a significant incident to the competent CSIRT:

– early warning of a significant incident

– initial notification of a significant incident

– interim report on a significant incident

– progress report

– final report on a significant incident.

Article 66

(1) Key and important entities are obliged to submit an early warning of a significant incident to the competent CSIRT, without delay, and no later than within 24 hours of becoming aware of the significant incident.

(2) An early warning of a significant incident must contain:

– date and time of incident discovery

– description of the basic features of the incident

– information on whether there is a suspicion that the significant incident was caused by illegal or malicious activity

– the entity's assessment of whether the incident may have a cross-border impact

– the entity's assessment of whether the incident may have a cross-sectoral impact.

Article 67

(1) Key and important entities are required to submit the initial notification of a significant incident to the competent CSIRT, without delay, and no later than 72 hours from the moment of becoming aware of the significant incident.

(2) The initial notification of a significant incident must contain:

– an updated description of the basic characteristics of the incident and other information submitted in accordance with Article 66 of this Regulation

– initial assessment of a significant incident

– indicators of compromise, if available.

(3) The initial assessment of a significant incident includes an assessment by the key and important entity of:

– which network and information system of the entity was affected by the incident and the importance of that system for the provision of services or the performance of the entity's activities

– the severity and impact of the incident, taking into account the extent to which the provision of services or the performance of the entity's activities is threatened, the duration of the incident and the number of service recipients affected by the incident

– technical characteristics of the incident

– vulnerabilities that are exploited

– the subject's experiences with similar incidents.

Article 68.

By way of derogation from Article 66, paragraph 1 of this Regulation and Article 67, paragraph 1 of this Regulation, trust service providers shall submit an initial notification of a significant incident to the competent CSIRT, without delay and no later than 24 hours from the moment of becoming aware of the significant incident, including information on the date and time of becoming aware of the incident.

Article 69

(1) Key and important entities are required to submit interim reports
report on a significant incident at the request of the competent CSIRT.

(2) In the request referred to in paragraph 1 of this Article, the competent CSIRT shall specify:

– to which data from Article 67 of this Regulation does the request relate?

– deadline for submitting an interim report on a significant incident.

(3) The deadline for submitting an interim report on a significant incident shall be determined depending on the scope and complexity of the data to which the request referred to in paragraph 1 of this Article relates, provided that the deadline set may not be shorter than 48 hours or longer than seven days from the receipt of the request for submission of an interim report.

(4) If it deems it necessary, the competent CSIRT may submit the requests referred to in paragraph 1 of this Article repeatedly, until the final report on the significant incident is submitted.

Article 70

(1) Key and important entities are required to submit the final report on a significant incident to the competent CSIRT no later than 30 days from the date of delivery of the initial notification of a significant incident.

(2) The final report on a significant incident must contain:

– detailed description of the incident

– the type of threat or root cause that likely caused the incident

– confirmed indicators of compromise

– information about a suspected or confirmed cyber attacker

– data on the severity and impact of the incident, which must include a description of the disruption caused by the incident in the provision of services or the performance of the entity's activities, the duration of the incident and the number of service recipients affected by the incident, and the possible compromise of sensitive data

– risk mitigation measures and mitigation measures applied
risks whose implementation is in progress

– measures to achieve a higher level of cybersecurity that the entity plans to implement in order to minimize the possibility of the same or similar incident recurring and to mitigate the risk

- data on the cross-border effect of the incident, if the incident had such an effect

– data on the cross-sectoral impact of the incident, if the incident had such an impact.

Article 71

(1) In the event that the incident is still ongoing, key and important entities are required to submit a progress report to the competent CSIRT, instead of a final report on a significant incident, within the deadline referred to in Article 70, paragraph 1 of this Regulation.

(2) The progress report must contain:

– an updated description of the basic characteristics of the incident, the initial assessment of the significant incident and other information submitted in accordance with Articles 67 to 69 of this Regulation

– the type of threat or root cause that likely caused the incident

– risk mitigation measures and mitigation measures applied
risks whose implementation is in progress

– assessment and explanation of the causes that led to the prolonged duration of incident response.

(3) In the event of a significant incident lasting longer than 60 days from the date of submission of the initial notification of a significant incident, key and important entities are required to submit a progress report to the competent CSIRT every 30 days.

(4) In the cases referred to in paragraphs 1 and 3 of this article, key and important entities are obliged to submit a final report on a significant incident to the competent CSIRT no later than 30 days after the last submitted progress report.

Article 72

(1) Notifications of significant incidents shall be submitted on forms established by the general guidelines for the implementation of the obligation to notify of significant incidents.

(2) The general guidelines referred to in paragraph 1 of this Article shall be adopted jointly by the competent CSIRTs, with the subsequent consent of the central state authority for cybersecurity.

(3) Forms and general guidelines from paragraph 1 of this article are drawn up taking into account ENISA's technical guidelines on information parameters for the purpose of notifying ENISA based on Article 42, paragraph 2 of the Act.

(4) The competent CSIRTs, after obtaining the consent of the central state authority for cybersecurity on the general guidelines referred to in paragraph 1 of this Article, shall publish the general guidelines on their websites.

Article 73

(1) Competent CSIRTs may issue sectoral guidelines for the implementation of the obligation to notify about significant incidents, if there are sectoral specificities that are not covered by the general guidelines from Article 72 of this Regulation.

(2) Competent CSIRTs publish the sectoral guidelines from paragraph 1 of this article on their websites.

Article 74

(1) On the implementation of the obligation of key and important entities related to the delivery of notifications of significant incidents to criminal prosecution bodies in cases referred to in Article 37, paragraph 3 of the Act, special guidelines are issued.

(2) The guidelines referred to in paragraph 1 of this Article shall be adopted jointly by the competent authorities.
nor CSIRTs, in cooperation with law enforcement authorities.

(3) The competent CSIRTs shall publish the guidelines referred to in paragraph 1 of this Article on their websites.

SECTION 3
PROCEDURES OF THE COMPETENT CSIRT REGARDING NOTIFICATIONS RECEIVED ABOUT SIGNIFICANT INCIDENTS

Article 75

If a notification of a significant incident has not been submitted in accordance with Articles 66 to 72 of this Regulation, the competent CSIRT will notify the entity and set a deadline within which the entity is obliged to eliminate the deficiencies, with a warning of legal consequences in accordance with the Act if it fails to do so within the given deadline.

Article 76

(1) The competent CSIRT shall, without delay, and no later than 24 hours from the receipt of an early warning of a significant incident, provide the entity with initial feedback on the incident.

(2) In addition to the initial feedback on the incident, the competent CSIRT will provide the key and important entity with guidelines and operational advice on the implementation of possible measures to mitigate the incident, if the entity has requested this in an early warning about a significant incident, i.e. an initial notification about a significant incident in the cases referred to in Article 68 of this Regulation.

(3) In the event that the entity is called upon in accordance with Article 75 of this Regulation to eliminate deficiencies in the delivered early warning about a significant incident, the deadline from paragraph 1 of this article is counted from the delivery of the corrected early warning about a significant incident.

(4) The deadlines referred to in paragraphs 1 and 3 of this Article in cases referred to in Article 68 of this Regulation shall be calculated from the receipt of the initial notification of a significant incident.

Article 77

Upon receipt of the notification referred to in Articles 67 to 71 of this Regulation, the competent CSIRT shall conduct an analysis and classification of the incident according to the national incident taxonomy and, if circumstances permit, upon receipt of such notification, shall provide key and important entities with information relevant for further handling of the significant incident, in particular information that could contribute to the effective resolution of the significant incident.

Article 78

The national taxonomy of incidents referred to in Article 77 of this Regulation shall be adopted by the central state authority for cybersecurity, upon the proposal of the competent CSIRTs.

Article 79

(1) The competent CSIRT is involved in the process of solving a significant incident at the request of a key and important subject.

(2) The request referred to in paragraph 1 of this article can be submitted by key and important entities within any of the stages of reporting on a significant incident referred to in Article 65 of this Regulation, using the reporting forms referred to in Article 72 of this Regulation.

(3) In the case referred to in paragraph 1 of this Article, key and important entities are obliged to provide the competent CSIRT, at its request, with all data necessary for the effective resolution of a significant incident.

(4) The submission of data pursuant to paragraph 3 of this Article shall not affect the implementation of the obligations of key and important entities referred to in Articles 65 to 72 of this Regulation.

Article 80

(1) Upon receipt of a notification referred to in Articles 66 to 72 of this Regulation on significant incidents with cross-border or cross-sectoral impact, the competent CSIRT shall, without delay and no later than three days from receipt of such notification, submit to the competent authority for the implementation of cybersecurity requirements a report on the possible cross-border and cross-sectoral impact of the significant incident, with an assessment of the potential impact of the incident.

(2) When preparing the report referred to in paragraph 1 of this Article, the competent CSIRT shall also take into account the information provided to it about the significant incident by the single point of contact and the competent authority for the implementation of cybersecurity requirements.

Article 81

The competent authority for the implementation of cybersecurity requirements shall, without delay, and no later than three days from the receipt of the report referred to in Article 80, paragraph 1 of this Regulation, provide a statement to the competent CSIRT on the assessment of the cross-border and cross-sectoral impact of the incident.

Article 82

(1) If it receives new information about a significant incident that has an impact on the previously given impact assessment of the incident, or when requested to do so by the competent authority for the implementation of cybersecurity requirements, the competent CSIRT is obliged to prepare a new report on the cross-border and cross-sectoral impact of the significant incident, with a new impact assessment of the incident.

(2) In the case referred to in paragraph 1 of this Article, Articles 80 and 81 of this Regulation shall be applied accordingly.

Article 83

The reports of the competent CSIRT from Articles 80 and 82 of this Regulation are delivered to the single contact point no later than three days after they are drawn up, and the declaration of the competent body from Article 81 of this Regulation is delivered to the single contact point no later than three days after receipt.

Article 84.

In carrying out the tasks referred to in Articles 75 to 83 of this Regulation, the competent CSIRT shall give priority to priority tasks according to the risk assessment.

CHAPTER II.
NOTIFYING SERVICE RECIPIENTS OF SIGNIFICANT INCIDENTS AND SERIOUS CYBER THREATS

Article 85

(1) Key and important entities are obliged, without delay, and no later than within 72 hours of becoming aware of a significant incident, to clearly and easily Inform recipients of its services who may be affected by a significant incident in a demonstrable manner.

(2) The notification referred to in paragraph 1 of this Article must contain the following: information about a significant incident:

– type and brief description of the incident

– cause of the incident

– possible impact of the incident on the service

– contact details of the entity

– instructions on the actions of service recipients for the purpose of mitigating the impact of the incident and compensation for the damage caused.

(3) In the event that at the time of sending the notification referred to in paragraph 1 of this Article, some of the data referred to in paragraph 2 of this Article are not known to the key and important entity, the entity shall be obliged to deliver the remaining data to the recipients of services that could be affected by such an incident, no later than 72 hours after sending the notification.

Article 86

(1) In the event of a serious cyber threat, key and important entities are obliged to inform the recipients of their services, who could be affected by such a threat, of all possible protective measures or legal remedies that they can use to prevent or compensate for the damage caused and, if necessary, inform the recipients of the services about the serious cyber threat itself.

(2) Article 85 of this Regulation shall be applied appropriately to the notification of service recipients about serious cyber-threats.

CHAPTER III.
NOTIFICATIONS OF KEY AND IMPORTANT ENTITIES ON A VOLUNTARY BASIS

Article 87

(1) When they voluntarily inform about other incidents on the basis of Article 39 of the Act, key and important entities submit a notification about the incident to the competent CSIRT, which must contain:

– date and time of incident discovery

– a description of the technical characteristics of the incident, including the duration of the incident and the type of threat or root cause that likely caused the incident

– indicators of compromise, if available

– data on vulnerabilities being exploited

– data on which network and information system of the entity was affected by the incident

– a description of the disruption caused by the incident in the provision of services or the performance of the entity's activities and the number of recipients of the entity's services and/or users of the entity's network and information system affected by the incident

– risk mitigation measures and mitigation measures applied
risks whose implementation is in progress

– the subject's experiences with similar incidents in the past

- information on whether there is a suspicion that the incident was caused by illegal or malicious activity.

(2) Key and important entities may submit the notification from paragraph 1 of this article to the competent CSIRT immediately upon becoming aware of the incident, and no later than within 30 days from the moment of learning about the incident, taking into account the seriousness of the incident and the extent of the data on the avoided incident available to the entity.

(3) From the moment of submitting the incident notification until the expiry of the deadline for its submission referred to in paragraph 2 of this Article, key and important entities may submit updated information referred to in paragraph 1 of this Article to the competent CSIRT.

Article 88.

(1) When voluntarily reporting cyber threats pursuant to Article 39 of the Act, key and important entities shall submit a cyber threat notification to the competent CSIRT, which must contain:

– date and time of discovery of the cyber threat

– description of the cyber threat and its current status

– data on the potential impact of the cyber threat on the entity's network and information systems and its users, including a description of the disruptions that the cyber threat could cause in the provision of services or the performance of the entity's activities

– description of measures implemented to prevent the impact of cyber-cyber threats to the entity's network and information systems.

(2) Key and important entities may submit the notification referred to in paragraph 1 of this article to the competent CSIRT immediately upon learning of a cyber threat, and no later than within 30 days from the moment of learning of the cyber threat, taking into account the seriousness of the cyber threat and the extent of the cyber threat data available to the entity.

(3) From the moment of submission of the cyber threat notification until the expiry of the deadline for its submission referred to in paragraph 2 of this Article, key and important entities may submit updated data referred to in paragraph 1 of this Article to the competent CSIRT.

Article 89

(1) When they voluntarily inform about avoided incidents on the basis of Article 39 of the Act, key and important entities submit a notification about the avoided incident to the competent CSIRT, which must contain:

– date and time of learning about the avoided incident

– a description of the technical characteristics of the avoided incident, including the type of threat or root cause that could have caused the incident

– indicators of compromise, if available

– data on vulnerabilities that were attempted to be exploited

– data on which network and information system of the entity is was exposed to an avoidable incident

– data on the potential impact of the avoided incident on the entity's network and information systems and its users, including a description of the disruptions that the avoided incident could have caused in the provision of services or the performance of the entity's activities

– the subject's experiences with similar avoided incidents in the past

– information on whether there is a suspicion that the incident was avoided caused by illegal or malicious activity.

(2) Key and important entities may submit the notification from paragraph 1 of this article to the competent CSIRT immediately upon learning of the avoided incident, and no later than within 30 days from the moment of learning about the avoided incident, taking into account the seriousness of the avoided incident and the extent of the avoided incident data available to the entity.

(3) From the moment of submission of the notification of an averted incident until the expiry of the deadline for its submission referred to in paragraph 2 of this Article, key and important entities may submit updated information referred to in paragraph 1 of this Article to the competent CSIRT.

Article 90

(1) Notifications about incidents, cyber threats and avoided incidents are submitted on the forms established by the guidelines for the implementation of voluntary notification.

(2) The guidelines referred to in paragraph 1 of this Article shall be jointly adopted by the competent CSIRTs, with the subsequent approval of the central state authority for cybersecurity.

(3) The forms and guidelines from paragraph 1 of this article are drawn up taking into account ENISA's technical guidelines on information parameters for the purpose of notifying ENISA based on Article 42, paragraph 2 of the Act.

(4) The competent CSIRTs, after obtaining the consent of the central state authority for cybersecurity on the adopted guidelines referred to in paragraph 1 of this Article, shall publish the guidelines on their websites.
pages.

Article 91

(1) On the occasion of the notification from Articles 87 to 89 of this Regulation, the competent CSIRT will deliver to the key and important entity recommendations and operational advice on the implementation of possible mitigation measures and effective resolution of the incident, prevention of the occurrence of the potential effect of a cyber threat and an averted incident, if the entity has requested this in the delivered notification of the incident, notification of the cyber threat or the averted incident.

(2) When the submitted data indicates that the reported event has the characteristics of a significant incident referred to in Articles 59 to 62 of this Regulation, the competent CSIRT shall provide the key and important entity with a notification of the obligation to notify of a significant incident in accordance with Articles 64 to 74 of this Regulation.

Article 92

(1) The competent CSIRT is involved in the procedure for resolving the incident of which it has been notified pursuant to Article 87 of this Regulation, if the subject has requested it in the submitted notification of the incident.

(2) In the case referred to in paragraph 1 of this Article, Article 79, paragraph 3 of this Regulation shall apply accordingly.

Article 93

When performing the tasks referred to in Articles 91 and 92 of this Regulation, the competent CSIRT shall give priority to priority tasks according to the risk assessment, and when processing notifications received from key and important entities pursuant to Articles 37 and 39 of the Act, it shall give priority to processing notifications of significant incidents.

CHAPTER IV.
NATIONAL PLATFORM FOR COLLECTION, ANALYSIS AND EXCHANGE OF DATA ON CYBER THREATS AND INCIDENTS

Article 94.

(1) Key and important entities are obliged to use the national platform for collecting, analyzing and exchanging data on cyber threats and incidents (hereinafter: the national platform) as the primary means of delivering information about:

– significant incidents in accordance with Article 37 of the Act and Articles 58 to 73 of this Regulation and

– other incidents, avoided incidents and cyber threats in accordance with Article 39 of the Act and Articles 87 to 90 of this Regulation.

(2) In exceptional cases when the delivery of notifications pursuant to paragraph 1 of this Article is not possible for justified reasons, key and important entities shall deliver the notifications referred to in paragraph 1 of this Article through the communication channels defined in the guidelines of the competent CSIRTs referred to in Article 72, paragraph 1 and Article 90, paragraph 1 of this Regulation.

Article 95

(1) Key and important entities acquire the status of a user of the national platform on the date of entry of the entity into the List of Key and Important Entities.

(2) The competent authorities for the implementation of cybersecurity requirements are obliged to inform the key and important entity in the notification on the categorization of entities referred to in Article 19, paragraph 1 of the Act about the acquisition of the status of a national platform user entity and the obligations arising for it from Articles 96 and 97 of this Regulation.

Article 96

(1) Key and important entities shall, within eight days of receiving the notification referred to in Article 95, paragraph 2 of this Regulation, appoint a person responsible for administering the entity's account on the national platform (hereinafter referred to as: administrator).

(2) Key and important entities are obliged to appoint an administrator from among their employees.

(3) Key and important entities may appoint up to two administrators strator.

(4) Data on appointed administrators, including changes in persons of administrators or individual data on appointed administrators, are entered into the national platform by key and important entities in accordance with the instructions that form an integral part of the notification from Article 19, paragraph 1 of the Act.

Article 97

(1) Key and important entities are obliged to appoint persons authorized to implement the notification referred to in Articles 37 and 39 of the Act (hereinafter: users of the national platform) within eight days of receiving the notification from Article 95, Paragraph 2 of this Regulation.

(2) Key and important entities may appoint users of the national platform from among their employees or employees of an external provider of related services in the entity, whereby the responsibility for implementing the notification from Articles 37 and 39 of the Act remains with the key and important entity.

(3) Key and important entities are obliged to determine the scope of their user rights in the decision on the appointment of users of the national platform in such a way as to determine:

- is the person responsible for the notification referred to in Article 37 of the Act and/or for the notification referred to in Article 39 of the Act

- type of services or activities of the subject from Annexes I and II. of the Act to which the debt referred to in subparagraph 1 of this paragraph refers.

(4) When determining the total number of users of the national platform, key and important entities shall take into account the size of the entity, its structure, the degree of exposure of the entity to risks and the likelihood of incidents occurring.

(5) The administrator can also be appointed as a user of the national platform.

Article 98

In the national platform, the administrator has the following powers: the entity for which it is appointed:

- entering users of the national platform and their user rights,

– updating data on users of the national platform and

– deactivation of users of the national platform

– deactivation of user rights.

Article 99

On the basis of the decision on the appointment of users of the national platform from Article 97 of this Regulation, within the framework of their user rights, the administrator of the national platform assigns the following powers to the users of the national platform of the entity for which he was appointed:

– entering notifications of significant incidents referred to in Article 37. Law and/or

– entering information about other incidents, cyber attacks accidents and avoided incidents referred to in Article 37 of the Act.

Article 100.

(1) Competent authorities for the implementation of cyber security requirements are obliged to notify the subject in the notification from Article 19, paragraph 3 of the Act, of the termination of the subject's status as a user of the national platform.

(2) The competent authority for the implementation of cybersecurity requirements shall also deliver the notification referred to in paragraph 1 of this Article to CARNET, in order to implement the deactivation of the user accounts of the administrator and user of the national platform for the entity to which the notification relates.

(3) CARNET is obliged to deactivate user accounts no later than three days after receiving the notification referred to in paragraph 1 of this Article.

Article 101.

(1) Key and important entities are obliged to use the national platform in accordance with the terms of use of the national platform contained in the guidelines for the use of the national platform.

(2) Guidelines for the use of the national platform are issued by CAR-NET, based on the previously obtained opinion of competent CSIRTs and competent authorities for the implementation of cyber security requirements.

(3) When determining and updating the terms of use of the national platform, CARNET is obliged to take into account the guidelines of the competent CSIRTs referred to in Article 72, paragraph 1 and Article 90, paragraph 1 of this Regulation.

(4) The terms of use of the national platform shall determine, among other things, the terms of use of the national platform in cases referred to in Article 59, paragraph 3 of the Act, in accordance with the protocol on the conduct of the competent authorities concluded for the entity.

Article 102.

(1) CARNET grants the competent authorities referred to in Annex III to the Act and the single point of contact access rights to the national platform and enables its use to the extent necessary for these authorities to carry out their tasks prescribed by the Act, namely:

– competent authorities for the implementation of cybersecurity requirements for the implementation of tasks referred to in Article 59, paragraphs 1 to 5 and Articles 64 and 65 of the Act

– competent CSIRTs for the implementation of the tasks referred to in Article 66. Law and

– a single point of contact for the implementation of tasks referred to in Articles 40 to 42 of the Act.

(2) The competent authorities referred to in Annex III to the Act and the single point of contact are obliged to inform CARNET of:

- employees responsible for administering the accounts of the superior body, i.e. the single point of contact on the national platform

– other employees of the competent authority or the single authority contact points authorized to use the national platform

- the scope of user rights for persons from sub-paragraphs 1 and 2 of this paragraph.

(3) In the cases referred to in Article 94, paragraph 2 of this Regulation, the competent authorities from Annex III. of the Act and the single point of contact achieves access to the submitted notifications of key and important entities in accordance with the guidelines of the competent CSIRTs from Article 72, paragraph 1 and Article 90, paragraph 1 of this Regulation.

Article 103.

(1) Data on an individual significant incident shall be kept in the national platform for 25 years from the date of submission of the final report on the significant incident referred to in Article 70 of this Regulation.

(2) Data on certain other incidents, cyber threats and avoided incidents are stored in the national platform for 15 years from the date of delivery of the notification from Articles 87 to 89 of this Regulation.

(3) Data on subjects who are users of the national platform, their administrators and users of the national platform are kept for 15 years from the date of deactivation of the subject's user account in accordance with Article 100 of this Regulation, provided that the retention periods for all significant incidents notified to the relevant CSIRT by the relevant subject have expired within that period.

(4) The competent CSIRTs are obliged, in accordance with the division of competences set out in Annex III to the Act, to delete data on significant incidents, other incidents, cyber threats and avoided incidents from the national platform after the expiry of the retention periods set out in paragraphs 1 and 2 of this Article.

(5) After the expiration of the retention period referred to in paragraph 3 of this article, CARNET is obliged to delete from the national platform the data on the subjects of users of the national platform, their administrators and users of the national platform.

PART SIX
IMPLEMENTATION OF INCIDENT NOTIFICATIONS AND CYBER THREATS AS VOLUNTARY MECHANISM OF CYBERNETICS PROTECTION

Article 104.

(1) Entities from Article 47, paragraph 1 of this Regulation who intend to use the possibility of reporting incidents and cyber threats based on Article 50, paragraph 2 of the Act, are obliged to inform the competent CSIRT of such intention.

(2) Attached to the notification referred to in paragraph 1 of this Article, the entity shall submit a declaration of compliance referred to in Article 35, paragraph 3 of the Act, which shall not be older than one year from the date of preparation of the notification referred to in paragraph 1 of this Article.

Article 105.

(1) Entities from Article 47, Paragraph 1 of this Regulation are obliged to conduct cyber security self-assessments at least once every two years as long as they use the option of reporting incidents and cyber threats pursuant to Article 50, paragraph 2 of the Act, and the prepared statements of compliance referred to in Article 35, paragraph 3 of the Act are required to be submitted to the competent CSIRT without delay, and no later than eight days from the date of their preparation.

(2) The deadline referred to in paragraph 1 of this Article shall be calculated from the date of preparation of the statement of compliance submitted to the competent CSIRT in accordance with Article 104, paragraph 2 of this Regulation, or from the date of preparation of the statement of compliance submitted to the competent CSIRT referred to in Article 35, paragraph 3 of the Act.

Article 106.

A significant incident in the sense of Article 50, paragraph 2 of the Act, about which entities from Article 47, paragraph 1 of this Regulation voluntarily inform the competent CSIRT, is any incident that meets at least one criterion for determining significant incidents from Articles 58 to 62 of this Regulation, taking into account the criterion thresholds, when they are prescribed.

Article 107.

(1) Articles 87 to 92 of this Regulation shall be applied accordingly to the notification of significant incidents, other incidents, cyber threats and avoided incidents based on Article 50 Paragraph 2 of the Act.

(2) Entities referred to in Article 47, paragraph 1 of this Regulation shall be obliged to submit notifications about significant incidents, other incidents, cyber threats and avoided incidents exclusively through the communication channels defined in the guidelines of the competent CSIRTs referred to in Article 90, paragraph 1 of this Regulation.

Article 108.

When processing notifications about significant incidents, other incidents, cyber threats and avoided incidents received pursuant to Articles 37, 39 and Article 50, paragraph 2 of the Act, the competent CSIRT shall give priority to processing notifications received pursuant to Articles 37 and 39 of the Act.

PART SEVEN
NATIONAL DETECTION SYSTEM CYBER THREATS AND PROTECTION CYBERSPACE

Article 109.

(1) Key entities, important entities and other entities not categorized as key or important entities may voluntarily implement a cyber protection measure by accessing the national system for detecting cyber threats and protecting cyberspace (hereinafter: the national system), if the central state authority for cybersecurity has assessed the entity as critical within the meaning of Article 52, paragraph 1 of the Act.

(2) For the purpose of carrying out assessments of the criticality of entities within the meaning of Article 52, paragraph 1 of the Act and deciding on priorities in the implementation of voluntary measures for the protection of access to the national system, the central state authority for cybersecurity shall classify entities according to risk categories.

Article 110.

(1) The assessment of the criticality of an entity within the meaning of Article 52, paragraph 1 of the Act is carried out on the basis of a request for accession to the national system submitted by the entity, or on the basis of a proposal for accession to the national system submitted by a state body.

administration or regulatory body competent for the sector to which the legal entity belongs.

(2) Requests and proposals for accession to the national system must contain information on:

– the services provided by the entity or the activities carried out by the entity in relation to other providers of the same or similar services and activities in the Republic of Croatia

– network and information systems used by the entity in providing services or performing activities and their exposure to risks, dangers and threats in cyberspace

– the manner in which the entity's network and information systems are designed, managed and maintained, as well as the relevant European and international standards and best security practices applied.

(3) In addition to the information referred to in paragraph 2 of this Article, proposals for accession to the national system must also contain a statement by the applicant on the reasons why it is proposed that the entity implement the cyber protection measure of accession to the national system.

(4) Requests and proposals for joining the national system shall be submitted to the central state authority for cybersecurity in accordance with the instructions published by the central state authority for cybersecurity on its website.

(5) The submitter of the proposal shall also notify the entity for which he submitted such a proposal about the submitted proposal for accession to the national system.

Article 111.

(1) The central state cybersecurity authority may, if necessary, request the entity for which an assessment is being conducted for the purpose of criticality of the entity for access to the national system to provide additional data on the entity's network and information systems.

(2) The entity shall submit the requested data to the central state authority for cybersecurity in accordance with the instructions referred to in Article 110, paragraph 4 of this Regulation.

Article 112.

(1) By way of derogation from Article 109 of this Regulation, ministries shall be obliged to implement the cyber protection measure of mandatory access to the national system.

(2) By way of derogation from Article 109 of this Regulation, other state administration bodies, state bodies and legal entities with public authority are obliged to implement the cyber protection measure of mandatory access to the national system when the following criteria are met:

– the entity is categorized as a key entity or

– is the central state body for cybersecurity assess-
of the subject as critical in the sense of Article 52, paragraph 1 of the Act.

(3) The assessment of the criticality of subjects from paragraph 2, sub-paragraph 2 of this article is carried out in connection with the proposal of the competent authority for the implementation of cyber security requirements for the public sector.

(4) The central state authority for cybersecurity shall be obliged to inform the entity about the fulfilment of the criteria referred to in paragraph 2, subparagraph 2 of this Article and about the obligation to join the national system.

Article 113.

(1) Regardless of whether it is implemented as a mandatory or voluntary cyber security measure, access to the national system shall be carried out on the basis of agreements concluded between the central state cybersecurity authority and the entity accessing the national system.

(2) The agreement referred to in paragraph 1 of this Article shall regulate:

– mutual rights and obligations of the central state body and the entity accessing the national system

– mutual conditions of data protection and confidentiality

– maintenance and protection of the national system software and tools

– technical and other conditions for accessing and using the national system.

(3) The agreements referred to in paragraph 2 of this Article shall be classified with the appropriate level of secrecy.

PART EIGHT

TRANSITIONAL AND FINAL PROVISIONS

Article 114.

(1) The single point of contact will issue guidelines from Article 31, paragraph 1 of this Regulation within 90 days from the date of entry into force of this Regulation.

(2) The central state authority for cybersecurity shall adopt the guidelines referred to in Article 40 of this Regulation within 90 days from the date of entry into force of this Regulation.

(3) The central state authority for cybersecurity shall adopt the guidelines referred to in Article 45, paragraph 3 of this Regulation within six months from the date of entry into force of this Regulation.

(4) The central state authority for cybersecurity shall prepare a correlation overview of the measures referred to in Article 49 of this Regulation within six months from the date of entry into force of this Regulation.

(5) The central state authority for cybersecurity shall adopt a national taxonomy of incidents referred to in Article 77 of this Regulation within 90 days from the date of entry into force of this Regulation.

(6) The central state body for performing tasks in the technical areas of information security shall adopt the guidelines referred to in Article 57 of this Regulation within six months from the date of entry into force of this Regulation.

(7) The competent CSIRTs shall adopt the guidelines referred to in Articles 72, 74 and 90 of this Regulation within 90 days of the date of entry into force of this Regulation.

(8) CARNET shall issue guidelines referred to in Article 101 of this Regulation in within 90 days from the date of entry into force of this Regulation.

Article 115.

On the day this Regulation enters into force, the Decision on measures and activities to increase national capabilities for timely detection and protection against state-sponsored cyber attacks, Advanced Persistent Threat (APT) campaigns and other cyber threats, class: 022-03/21-04/91, registration number: 50301-

29/09-21-2, from April 1, 2021.

Article 116.

This Regulation shall enter into force on the eighth day following its publication in the Official Gazette, except for the provisions of Articles 104 and 105 of this Regulation, which shall enter into force on 1 January 2026.

Class: 022-03/24-03/108

Reg. No.: 50301-29/23-24-5

Zagreb, November 21, 2024.

President

Andrej Plenkoviÿ, M.Sc., mp

ANNEX I

LIST OF ACTIVITY SECTORS1

A. LIST FOR APPENDIX I OF THE LAW - SECTORS OF HIGH CRITICALITY

Sector	**Subsector** 1.	**Subject type**
Energy	(a) electric energy	– electricity entities –
		distribution system operators
		– transmission system operators
		– electricity producers
		– nominated electricity market operators – market
		participants providing energy aggregation, demand response or storage services
		– charging point operators who are responsible for the management and operation of charging points that provide end-users with a supply service, among others on behalf of and for the account of mobility service providers
	(b) central heating and cooling	– operator of a centralized heating or centralized cooling system
	(c) oil - oil pipeline operators	
		– operators of oil production, refineries and factories, as well as its storage and transportation
		– central stockpiling bodies
	(d) gas	– gas suppliers, including suppliers with public service obligations
		– distribution system operators
		– transport system operators
		– gas storage system operators
		– UPP terminal operators
		– natural gas companies
		– operators of natural gas refining and processing facilities
	(e) hydrogen	– operators of hydrogen production, storage and transfer
2. Traffic	(a) air traffic	– airlines
		– airport managing bodies, airports, including base airports, and bodies managing auxiliary facilities at airports
		– traffic management control operators providing air traffic control (ATC) services
	(b) railway transport	– infrastructure managers
		– railway carriers, including service facility operators
	(c) water transport	– passenger transport companies on inland waterways, at sea and along the coast, not including individual vessels operated by these companies
		– port management bodies, including their ports, and entities managing port facilities and equipment
		– service for the supervision and management of maritime traffic (VTS)
	(d) road traffic	– road authorities responsible for the control of traffic management, except for public entities for which traffic management or the operation of intelligent traffic systems is not a core part of their general activity
		– intelligent traffic system operators
3. Banker-thing		– credit institutions
4. Financial market infrastructure		– trading venue operators
		– central counterparties (CCPs)
5. Healthcare		– healthcare providers
		– reference laboratories
		– entities carrying out research and development activities for medicines – entities producing basic pharmaceutical products and pharmaceutical preparations from Area C of Section 21. National classifications of activities 2007 - NKD 2007 ("Narodne novine", no. 58/07 and 72/07)
		– entities that manufacture medical products considered essential during a public health emergency (“list of essential medical products in the event of a public health emergency”)
6. Water for human consumption		– suppliers and distributors of water intended for human consumption, excluding distributors for whom the distribution of water for human consumption is not a key part of their general activity of distributing other goods and products
7. Wastewater		– undertakings that collect, dispose of or treat municipal wastewater, sanitary wastewater or industrial wastewater, excluding undertakings for which the collection, disposal or treatment of municipal wastewater, domestic wastewater or industrial wastewater is not a core part of their general activity
8. Digital infrastructure		– Internet traffic exchange providers

[1] The types of entities marked with * are entities that are also obliged to submit data on the categorization of entities and obliged to submit data for maintaining a special register of entities.

		– DNS service providers, except root name server operators*
		– registry of national top-level Internet domain names*
		– cloud computing service providers*
		– data center service providers*
		– content delivery network providers*
		– trust service providers
		– providers of public electronic communications networks
		– providers of publicly available electronic communications services
9. ICT Service Management (B2B)		– managed service providers*
		– Managed security service providers*
		– information intermediaries as defined by the regulation governing the exchange of electronic invoices between entrepreneurs
10. Public sector		– state administration bodies – other state bodies and legal entities with public authority – private and public entities that manage, develop or maintain the state information infrastructure in accordance with the law governing the state information infrastructure
		– local and regional self-government units
11. Space		- terrestrial infrastructure operators owned, operated and managed by Member States or private parties and supporting the provision of services in space, excluding providers of public electronic communications networks

B. LIST FOR ANNEX II. OF LAW - OTHER CRITICAL SECTORS

Sector	Subsector	Subject type
1. Postal and courier services		– postal service providers
		– courier service providers
2. Waste management		– entities engaged in waste management, excluding entities for which waste management is not the main economic activity – entities engaged in the
3. Manufacturing, production and distribution of chemicals		manufacture of substances and the distribution of substances or mixtures – entities
		engaged in the production of products from substances or mixtures
4. Production, processing and distribution of food		– food businesses, which are engaged in wholesale and industrial production and processing
5. Production	(a) production of medical products and in vitro diagnostic medical products	- subjects that produce medical products and subjects that produce in vitro diagnostic medical products, except subjects that produce medical products listed in point 5. fifth indent of the List for Annex I of the Law - Sectors of high criticality
	(b) production of computers and electronic and optical products	– manufacturers of computers and electronic and optical products
	(c) production of electrical equipment	– electronic equipment manufacturers me
	(d) manufacture of machinery and equipment, n.e.c.	– manufacturers of machinery and equipment nec
	(e) production of motor vehicles, trailers and semi-trailers	– manufacturers of motor vehicles, trailers and semi-trailers
	(f) manufacture of other means of transport	– manufacturers of other means of transport
6. Digital service providers		– online marketplace providers*
		– Internet search engine providers*
		– social media platform providers*
7. Research		– research organizations
8. Education system		– private and public entities from the education system

C. LIST FOR SUBJECTS NOT INCLUDED IN THE APPENDICES OF THE LAW

1. Critical entities – entities that have been determined as critical entities based on the law governing the area of critical infrastructure.

2. Registrars2 – entities that provide domain name registration services, i.e. legal or natural persons performing independent activities authorized to register and administer .hr domains on behalf of the registry of national top-level Internet domains.

2 Included in the list of sectors of activity exclusively as obligees to submit data for keeping a special register of entities.

ANNEX II.

CYBER SECURITY MANAGEMENT MEASURES RISKS

1. Commitment and responsibility of persons responsible for the implementation of cyber security risk management measures

Objective: The objective of the measure is to ensure that persons responsible for managing the measures referred to in Article 29 of the Act (hereinafter: persons responsible for managing the measures) recognize cybersecurity as a key aspect of the entity's business and actively participate in managing cybersecurity and improving the level of cybersecurity in the entity through the integration of cybersecurity into strategic plans and decisions about the entity's business.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

1.1. define and adopt a strategic cyber security policy act by the entity's management body that defines the entity's goals in cyber security matters, cyber security risk management measures that the entity will apply, the organizational system and the distribution of roles, responsibilities and obligations, and that describes the cybersecurity management processes in the entity. The entity is obliged to review the established cyber security risk management measures at least once a year and assess their effectiveness, and update the strategic cyber security policy act as necessary

1.2. ensure that all employees of the entity and relevant legal entities with whom the entity has a business relationship, such as its suppliers or service providers, are informed of the main strategic guidelines of the cybersecurity policy that apply to them

1.3. ensure the necessary resources for the effective implementation of cyber security risk management measures, including financial resources, technical tools and human resources with the necessary expertise. In order to ensure continuity in the implementation of appropriate cyber security risk management measures and maintain a high level of their effectiveness, the entity will assess the necessary resources at least once a year and adjust them if necessary

1.4. establish, document and maintain active roles and responsibilities for cybersecurity in accordance with the size of the entity and its network and information systems and, as necessary, update the established roles and responsibilities in the entity. Given the size of the entity, roles in cybersecurity matters may be assigned to individuals within the entity with dedicated roles exclusively in cybersecurity matters (special roles) or they may be assigned to employees within their existing roles in the entity

1.5. it is necessary to separate individual roles in cyber security issues that could result in a potential conflict of interest (for example, separate roles for conducting risk assessments and roles for implementing measures)

1.6. appoint a dedicated person who is operationally responsible for cyber security at the level of the entire subject and to whom it is adequate access to persons responsible for implementing measures in the entity is ensured

1.7. ensure annual reporting to persons responsible for implementing measures on the state of cybersecurity. These reports should contain an analysis of established cybersecurity risk management measures, identified cyber threats and risks, and recommendations for improving the level of cybersecurity. Regular reporting should ensure that persons responsible for implementing measures are informed and enable strategic decisions to be made to raise the level of cybersecurity

1.8. define and provide security metrics on the state of cyber security, necessary for reporting to persons responsible for the implementation of measures in the subject, i.e. define key security metrics that will enable precise monitoring of the state of cyber security.

These metrics should include indicators that involve monitoring and collecting data such as the number and type of incidents, response times, and the percentage of compliance with prescribed cybersecurity risk management measures. Regular collection and analysis of this data should ensure quality reporting to those responsible for implementing the measures.

1.9. ensure appropriate activities necessary to raise awareness among persons responsible for implementing cybersecurity measures, particularly in matters of cybersecurity risk management and the potential impact of these risks on the services provided by the entity or the activity it performs. These activities include educational workshops, seminars and other forms of education on current cyber threats, best cybersecurity practices, and the importance of taking proactive cybersecurity risk management measures. This subset of cybersecurity risk management measures should ensure that the entity's management body is informed and continuously engaged in achieving and maintaining a high level of cybersecurity

1.10. ensure adequate mechanisms for the participation of persons responsible for implementing measures in cybersecurity initiatives and the promotion of continuous improvement of cybersecurity. These mechanisms include regular meetings, working groups and committees dedicated to cybersecurity issues, and a transparent flow of information between the cybersecurity operational team and the entity's management body. This subset of cybersecurity risk management measures should ensure the involvement of persons responsible for implementing measures in decision-making and setting priorities in the area of cybersecurity

1.11. provide adequate mechanisms for monitoring the main indicators of the state of cyber security in practically real time. These mechanisms include the implementation of advanced monitoring systems, automatic alarms and dashboards, which enable continuous monitoring and rapid detection of potential cyber threats. In this way, a timely reaction to incidents and minimization of the potential impact of incidents is enabled.

Measures 1.1 to 1.11 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures
cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure										
	1.1	1.2	1.3	1.4	1.5	1.6 1.7 CA		1.8	1.9	1.10	1.11
basic	A	A	A	A	C			C	C	C	C
intermediate	AND	AND	AND	AND	AND	AND	AND	AND	AND	C	C
advanced	AND	AND	AND	AND	AND	AND	AND	AND	AND	AND	C

2. Software and hardware asset management

Objective: The objective of the measure is to establish a structured approach to the identification and classification of the subject's software and hardware assets and to establish complete control and protection of the subject's software and hardware assets during their use, storage, transportation and ultimately deletion or destruction, i.e. life cycle management of software and hardware assets.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

2.1. The act adopted by the persons responsible for managing the measures shall define the rules and responsibilities for the management of software and hardware assets and establish criteria for establishing an "inventory of critical software and hardware assets" (hereinafter: critical asset inventory). This includes the development and documentation of details such as: who is responsible for various aspects of asset management, how assets should be classified into critical and other assets, or into multiple groups or categories in terms of their criticality for the entity's operations, and the procedures implemented for regular monitoring and maintenance of assets. The entity may define several clearly identifiable groups or categories of assets according to their criticality (for example, "infrastructure", "business applications", "support applications", "test systems" or "publicly available services", "internal services" or "production", "test", "development" or a combination of similar categories). The entity must then determine by this act which groups or categories represent critical software and hardware assets, whereby it is possible to define only the category of critical software and hardware assets, which then necessarily includes: email servers, VPN devices, security devices, as well as other software and hardware equipment according to the criticality assessment carried out by the entity. The entity must define the criteria for establishing an inventory of critical assets within the framework of this procedure (for example, all assets marked as "infrastructure" or as "business applications", or in the case of choosing to use multiple categories simultaneously, critical assets can be defined as "all publicly available services", "complete infrastructure" and "all business applications in production"). The classification of an entity's software and hardware assets may, for example, be based on requirements for the availability, authenticity, integrity and confidentiality of the assets, but must take into account the risks to which the assets are exposed and the importance of the assets to the entity's operations (as in the previous examples), because the ultimate goal is not the classification of the assets themselves, but rather enabling the entity to apply different measures to different categories of assets, in accordance with the different risk profiles that the entity assesses.

2.2. create a detailed inventory of critical assets that will contain all the information necessary for effective management and ensure its updating to a level that enables effective operational asset management and the implementation of adequate measures and controls.
The level of detail of the inventory of critical assets must be at a level that meets the business needs of the entity, and the inventory should include at least the following:

ÿ list of network and information systems used by the entity when providing services or performing activities

ÿ a list of key elements of network and information systems that are assessed as critical for maintaining the continuity of the entity's business

ÿ a unique identifier for each individual asset (for example inventory number, name or FQDN – Fully Qualified Domain Name)

ÿ location of the property

ÿ the responsible person and organizational unit of the entity or external service provider

2.3. determine the entity's critical data, taking into account the requirements for availability, authenticity, integrity and confidentiality of the data and taking into account the risks to which the data is exposed, as well as the significance of the data for the entity's business. The entity may define several clearly identifiable groups or categories of critical data (for example, all data that constitutes a trade secret, personal data, classified data or other data that the entity assesses as critical based on their importance for the entity's business)

2.4. define rules for using removable media for storing critical data, which all employees should be familiar with, and these rules should ensure that removable media is used exclusively for business purposes, prevent the execution of program code from removable media, and ensure automatic checking for malicious content on them, and when necessary, the use of appropriate encryption.

2.5. determine whether critical program and circuit assets are used exclusively on the subject's premises or are also used outside the subject's premises, and define the responsibilities for their preservation, use and return, when they are used outside the subject's premises

2.6. expand the inventory of critical assets with less critical software and hardware assets, i.e. with other groups or categories of assets, for entities that classify assets according to point 2.1 into multiple groups of critical software and hardware assets, with the aim of increasing the scope of risk assessment on assets that may affect the protection of critical assets and enabling the expansion of the application of additional protection measures, depending on the classification of asset criticality (for example, expand the categorization with "test systems", given that they are publicly available to third parties participating in their development)

2.7. establish the implementation of regular activities for the timely replenishment and updating of the inventory of critical assets in such a way that: a) updating the inventory of critical assets is an integral part of the process of acquiring new program and structural assets, including procurement to replace previously acquired assets, or b) introduce adequate automation in such a way that it is not possible to introduce changes to program and structural assets without updating the inventory of critical assets

2.8. implement detailed procedures and adequate technical measures for the safe disposal, safe transport of assets containing critical data, using generally known and proven methods for the safe disposal or deletion of data from devices and data storage media, and ensure measures to protect devices and data storage media in the event of transport. One-time transport of equipment or media may be protected by compensatory measures such as storage in secure containers, extraordinary transport monitoring or similar, while equipment intended for frequent transport or mobile devices of any type must have and use built-in and inseparable protection mechanisms such as encryption of storage media. If the described technical measures cannot be applied, software and hardware assets or data may be taken outside the entity's premises only after appropriate approval by the persons responsible for managing the measures

2.9. implement mechanisms for physical identification and marking of physical assets for data processing depending on the amount and spread of the same, which may include monitoring and monitoring of assets in real time using automation using the Internet of Things (IoT) and radio frequency identification (Radio Frequency Identification - RFID).

Measures 2.1 to 2.9 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure								
	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.
basic	AND	AND	AND	AND	AND	C	C	C	C
intermediate	AND	AND	AND	AND	AND	AND	AND	C	C
advanced	AND	AND	AND	AND	AND	AND	AND	AND	AND

3. Risk management

Objective: The objective of the measure is to establish an appropriate organizational framework for risk management so that the entity can identify and respond to all risks that threaten the security of its network and information systems and thereby pose a risk to the entity's operations.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

3.1. develop, document, implement and annually update a risk management process that includes risk assessment (identification, analysis, evaluation), determination of the level and criticality of risks, methods of risk treatment, identification of risk owners and their areas of responsibility. The entity must document, communicate and make available to the entity's employees, who are responsible for the business segments of the entity related to risks, cybersecurity policies and instructions on basic procedures for identifying, analyzing, assessing and treating risks, especially for individual risks that may lead to disruptions in the availability, integrity, authenticity and confidentiality of the entity's network and information systems

3.2. Conduct a risk assessment of assets from the critical asset inventory based on the principle of assessing all types of risks (all-hazards approach) and determining the level of each individual risk.

Given that cyber threats can have different origins, the risk assessment should be based on an approach that includes all hazards to software and hardware assets, including physical threats such as theft, fire, flood, natural phenomena, malfunctions, failure of electronic communications infrastructure, power outage or unauthorized physical access and damage to property, but also includes all threats that could jeopardize the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services. Special attention should be paid to risks arising from the use of third-party services. It is possible to use a risk assessment approach based on the described approach of identifying operational risks for assets from the entity's inventory (Asset-based approach), as well as an approach based on scenarios and identifying sources of strategic risks for the entity's business (Event-based approach)

3.3. Identified risks must be documented and a response to the identified risks defined, proportional to their level and criticality, which includes taking appropriate and proportionate technical, operational and organizational risk management measures.

As part of their risk assessment, entities should undertake and prioritize cybersecurity risk management measures commensurate with the degree of exposure of their business to risks and the likelihood of incidents occurring and their severity for the entity's business, including the potential social and economic, or cross-sectoral or cross-border impact of these risks.

3.4. implement detailed methods for analyzing and assessing risks and reporting on those risks. The entity must ensure regular reporting on identified risks, including any changes in risk assessments and proposed measures to mitigate or eliminate them. Reports must be provided to relevant business segments within the entity, to enable the provision of information peaceful decisions on cyber security risk management measures that are taken and the need to update the entity's strategic documents in cyber security matters

3.5. maintain a register of identified risks. This register should contain detailed information on all identified risks, including a description of the risk, an assessment of the probability and potential impact of the risk, and the current status and measures taken to address the risk. The register must be updated regularly to reflect identified new risks and changes in existing risks. The entity must also ensure that all relevant business segments within the entity are informed of the content and changes in the register of identified risks, in order to enable effective risk management and informed decisions on the necessary measures to manage cybersecurity risks

3.6. ensure that a risk assessment is carried out when implementing solutions that increase the area of exposure of the subject's network and information system to cyberattack, expand risks or introduce into use in the subject previously unknown architectures of network and information systems or protection measures. This assessment should include the identification of new threats and vulnerabilities arising from the implementation of new technologies or solutions, and an analysis of their potential impact on the overall cybersecurity of the subject. Based on the results of the assessment, the subject must take appropriate measures to mitigate the identified risks before implementing the solutions described in the introduction. All activities and results related to the risk assessment must be documented and reviewed by the relevant persons responsible for the subject's security issues

3.7. use advanced software tools for risk assessment and monitoring. These tools should enable detailed analysis and assessment of cybernetic threats, identification of vulnerabilities, and monitoring of incidents in real time. Software tools must be capable of automated collection and analysis of relevant data, generating reports and providing recommendations to mitigate or eliminate risks.

The entity must ensure regular use and updating of these tools to ensure their effectiveness in identifying and managing risks. The results obtained from the use of these tools must be integrated into the overall risk management process within the entity.

3.8. integrate risk management as part of enterprise risk management (ERM).

CONDITION: Measure 3.8. is mandatory for an entity that has established risk management processes at the entity's business level, in which case risk management, described within the subsets of measure 3. (3.1. to 3.7.), is implemented in an integrated manner, as part of the entity's established risk management process. If the entity does not have established risk management procedures at the entity's business level, it establishes measure 3. (3.1. to 3.7.) as a new business process.

Measures 3.1 to 3.8 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures
cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure							
	3.1.	3.2.	3.3.	3.4.	3.5.	3.6.	3.7.	3.8.
elementary	AAAAAAC secondary						CB	
	AAAAAA advanced AAAAAA						CB	
							CB	

4. Security of human resources and digital identities

Objective: The objective of the measure is to establish a structured approach that enables the entity to effectively manage the recruitment of appropriate human resources and manage the access rights of employees and external personnel to the entity's network and information systems.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

4.1. develop, document, implement and regularly maintain human resources security rules, taking into account all users of network and information systems, including external collaborators. Responsibilities related to cybersecurity are determined depending on the assigned roles of system users, determined according to the business needs of the entity. Entities must ensure that:

ÿ all employees of the entity understand their responsibilities in cybersecurity matters and apply basic cyber hygiene practices

ÿ all persons with administrative or privileged access to the entity's network and information system are aware of their increased responsibility and are committed to carrying out their roles and authorities assigned according to the entity's cybersecurity policy

- persons responsible for managing measures in the entity understand their role, responsibilities and powers

4.2. check the suitability and qualifications of candidates before their employment in accordance with the importance of the position for which the person is employed and applicable regulations (e.g. reference checks, verification of the validity of certificates, diplomas and degrees held, written tests, certificates of good conduct, etc.). It is necessary to determine for which roles, responsibilities and authorities in the entity it is necessary to check the suitability and qualifications of candidates before employment, or to require, for example, periodic submission of certificates of good conduct. Candidate screening must be conducted in accordance with applicable laws, regulations and ethics and must be proportionate to business requirements, aligned with access requirements for specific types of data and identified risks.

4.3. for all employees whose regular work responsibilities include designing, implementing, supervising or reviewing cybersecurity risk management measures, provide specific and documented training immediately upon the person's employment, as well as ongoing training of all such existing employees throughout their employment, in order to ensure an adequate level of knowledge about new technologies and cyber threats.
The entity must establish a training program in accordance with the entity's cybersecurity policy, subject-specific policies and relevant cybersecurity procedures within the entity's network and information systems. The training must include the necessary skills, expertise and knowledge for specific positions and the criteria for determining the training required for specific roles (for example, IT administrators must undergo additional training on secure configurations of the entity's software and hardware assets). The training program should include topics such as:

ÿ common and documented instructions relating to the secure configuration and operation of the entity's network and information systems, including mobile devices

ÿ regular and documented information on known cyber threats

ÿ usual and documented incident handling

4.4. provide regular training on basic cyber hygiene practices and awareness of risks and cyber threats for all employees, immediately upon employment with the entity and regularly thereafter during employment. The entity must establish an awareness program in accordance with the cybersecurity policy, subject-specific policies and relevant cybersecurity procedures within the entity's network and information systems. Awareness must cover basic IT skills and knowledge (for example, all employees must undergo training in the safe use of email and Internet browsing). The awareness program should include topics such as:

ÿ common and documented instructions relating to the security of IT systems and personal IT assets, including mobile devices

- safe use of authentication tools and credentials (for example, avoiding using the same passwords on different public services and avoiding using official addresses on public services in order to reduce the risk of attacks, avoiding saving passwords in web browsers, etc.)

- recognition and reporting of the most frequent incidents

4.5. define adequate disciplinary measures for employees in case of non-compliance with relevant cybersecurity rules depending on the employee's workplace, all in accordance with the applicable legal framework. When determining violations of work obligations and determining disciplinary measures for violations of the entity's cybersecurity policies, all applicable regulations, as well as specific contractual or other business requirements, are taken into account

4.6. ensure that each user of the network and information system (regardless of whether or not they are an employee of the entity), wherever technically possible and the system allows, has one or more digital identities that are theirs alone and uses them when working on the network and information systems of the entity. If the system does not allow the creation of an adequate number of digital identities or it is unreasonably expensive, some users may use the same digital identities only if the entity provides a compensatory measure that ensures unambiguous and demonstrable records of the use of shared digital identities (for example, group use of an institutional email address). The entity must:

ÿ create unique digital identities for users and network and information systems

- for users, a digital identity must be associated with a unique person so that the person can be held responsible for the activities carried out with that specific identity

ÿ enable monitoring of digital identity systems

ÿ keep records of digital identities and ensure monitoring i documenting all changes

ÿ digital identities assigned to multiple individuals (e.g. group email accounts) may only be permitted when necessary for business or operational reasons, and must be specifically approved and documented, with a compensatory recordkeeping measure in place that ensures data on each individual user and the time of use of such a digital identity

4.7. Cybersecurity responsibilities should be defined according to clear employee work roles and with alternates for each role. Employee access rights to the entity's network and information systems should be implemented in accordance with assigned business responsibilities and with the application of the "first in, first out" princ

"need-to-know", "least privilege" and "segregation of duties"

4.8. ensure the implementation of a clear and effective process that will ensure that the digital identities of all users of the network and information system are assigned in a timely manner and are changed or revoked in a timely manner due to organizational or business changes. This process must ensure the timely assignment of digital identities to new users and their rapid revocation when they are no longer needed. Access rights must be recorded and regularly reviewed and adjusted in accordance with organizational or business changes, thereby minimizing the risk of unauthorized access and protecting the entity's critical data

4.9. develop and implement incident response training within the entity for key personnel involved in the process. The training must include practical scenarios and regular exercises to ensure that all participants are well prepared to respond effectively to incidents. By regularly updating the training, the entity is obliged to adapt the training to new threats and best practices in the field of cybersecurity. This increases the entity's resilience to incidents and ensures a quick and adequate response in the event of their occurrence.

4.10. use digital distance learning systems for continuous training and certification of its personnel in the field of cybersecurity, especially in matters of managing cybersecurity risks and their impact on the services provided by the entity or the activity it performs. The entity may also opt for digital distance learning due to the simplicity of the training implementation, regardless of whether it is possible to organize live training.

4.11. implement social engineering testing, phishing simulations, and awareness programs. These activities must be regular and include all employees of the entity to identify vulnerabilities and educate staff on how to recognize and respond to such vulnerabilities. Awareness programs should include educational materials, workshops, and practical exercises.

This strengthens the security culture within the entity and reduces the risk of successful social engineering attacks

4.12. integrate the system for record keeping and human resources management with systems for managing digital identity and access rights to the network and information system, in order to ensure effective management of digital identities and access rights in real time. The entity is obliged to:

ÿ grant and revoke access rights based on the "need-to-know" principle, the "least privilege" principle and, as appropriate, the "segregation of duties" principle

ÿ ensure that access rights are reviewed in the event of termination or other change in employment status (e.g. termination or change of access rights, deactivation of user accounts, etc.)

ÿ ensure that access rights are appropriately granted to third parties, such as direct suppliers or service providers, taking into account the application of the principles set out in point 1 of this subset of measures. It is particularly important to limit such access rights, both in scope and duration.

ÿ keep a register of assigned access rights by user and

ÿ use access logging when managing access rights on the network and information system.

Measures from 4.1 to 4.12 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure											
	4.1.	4.2.	4.3.	4.4.	4.5.	4.6. 4.7.		4.8.	4.9.	4.10.	4.11.	4.12.
basic	AND	AND	AND	AND	AND	AND	AND	AND	C	C	C	C
intermediate	AND	AND	AND	AND	AND	AND	AND	AND	AND	AND	C	C
advanced	AND	AND	AND	AND	AND	AND	AND	AND	AND	AND	C	AND

5. Basic cyber hygiene practices

Objective: The objective of the measure is to ensure the implementation of basic security settings, rules and procedures for all employees and network and information systems of the entity that ensure the protection of the entity's network and information systems and its data, with the focus on preventing the most common types of incidents that occur as a result of malicious system infection, phishing attacks, improper and incorrect system configuration or the use of weak passwords.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

5.1. develop, document, maintain and implement basic cyber hygiene practice rules and regularly educate all users of their network and information systems about these rules

5.2. ensure that on all network and information access systems that use passwords, policies of the "strongest possible passwords" are used as a means of authentication, or if this is not possible due to operational reasons, the subject will define and justify its password policy, which must be in accordance with current good practices, such as the "Password Policy Guide of the Center for Internet Security (CIS)". If the entity has decided to implement its password policy, it should include various

Read the guidelines for different network and information systems and the purposes of using passwords, given that the level of protection required is often not the same on all types of network and information systems (for example, on newer Windows Server systems, using a password longer than 14 characters disables the use of outdated LAN Manager authentication). In general, on all network and information systems that do not have the option of multi-factor authentication (MFA) or for user accounts on which MFA is not technically possible, the minimum length is 14 characters, which must represent a combination of uppercase and lowercase letters, digits, and special characters. Passwords for user accounts with privileged access rights to the network and information system should be at least 16 characters long, and passwords for service accounts should be at least 24 characters long, using the previously described rule on the combination of uppercase and lowercase letters, digits, and special characters. For user accounts, including those with privileged access rights and service accounts, for which second-factor authentication is enabled, the password length may be shorter, but not shorter than 8 characters, if technically feasible, taking into account the need to use the previously described rule on the combination of uppercase and lowercase letters, digits and special characters. In the event that the network and information system cannot support the application of the described password determination rules, the entity is obliged to provide other compensatory measures for

protect, i.e. restricting access to the network and information system based on an appropriate compensatory measure (for example, mandatory restriction of physical access or mandatory remote access protected by two authentication factors). If the entity has opted for authentication that does not include the use of passwords, the use of two factors is necessary (biometrics and possession of another authentication device or managed access device). Within this subset of measures, the entity is obliged to:

ÿ ensure that the strength of authentication is appropriate to the criticality of the network and information system and in line with the risk assessment

- implement the use of authentication methods (passwords, digital certificates, smart cards, biometrics, etc.) that are in line with the state of technology development and use unique authentication means (something the user knows, such as a password or pin, something the user owns, such as a smartphone or token, and something the user is, such as a fingerprint, face recognition, etc.)

ÿ ensure the secure allocation and use of authentication means (e.g. storing and transferring such means in a protected form, automatic generation, creation of cryptographic digests with “salting” and/or “peppering”, etc.), which includes advising staff on appropriate procedures

ÿ request an initial change of personal access data (password and PIN) when using the user account for the first time, as well as in the event of suspicion that personal access data has been compromised

ÿ if technically feasible, it is necessary to prohibit the storage of passwords in web browsers

ÿ ensure account lockout after excessive failed login attempts, with the option of automatic unlocking after a reasonable period of time to prevent denial of service attacks

ÿ shut down inactive user sessions after a pre-defined a period of inactivity where the business process allows it i

ÿ require special credentials to access privileged or administrator user accounts

5.3. in addition to implementing a password policy, implement multi-factor authentication (MFA) for critical network and information systems that are more exposed to potential cyber attacks.
MFA is required for VPN access, SaaS tools accessible from the Internet, etc. It is necessary to ensure that usernames and passwords used on services with two-factor authentication are not used on other services without two-factor authentication. The strength of authentication must be aligned with the risk and exposure assessment of the network and information system. Multi-factor authentication should be considered when accessing critical network and information systems from a remote location, user and network and information system administration systems, critical subject data, etc. Multi-factor authentication can be combined with other techniques to require additional factors in specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device, or at an unusual time.

5.4. ensure the use of basic antivirus tools on all workstations. The use of software antivirus tools for malware detection and recovery is often not enough, so, in accordance with the risk assessment carried out by the entity, it is necessary to apply additional measures, i.e. use tools for detecting and responding to cyber threats at endpoints (EPP/EDR), with an appropriate level of automated response to threats, for the purpose of advanced protection on all workstations and servers where technically feasible. The entity may, due to technical complexity or very high implementation costs, decide to apply the measure only to a selected and justified subset of software or hardware assets in accordance with the risk assessment, for example on the server infrastructure, but then it must be logically separated from unprotected software and hardware assets, so that compromise of unprotected software and hardware assets would not easily lead to compromise of the protected part of the software and hardware assets

5.5. ensure timely and comprehensive application of security patches to the entity's entire software and hardware assets, as soon as they become applicable, or it is necessary to develop, define, document and implement a different vulnerability management process on the network and information systems used, which will ensure triage, assessment and prioritized and documented gradual application of security patches. If the entity decides not to immediately apply all security patches but to implement its own security patch application policy, it must, when defining the internal deadline for applying security patches, take into account the criticality and exposure factors of the network and information system, the severity of the discovered vulnerability, i.e. the criticality of applying the security patch, and the general state of cybersecurity and any current cyber attacks that exploit the vulnerabilities in question. In doing so, entities are required to establish and implement procedures that will ensure the following:

ÿ security patches are properly checked and tested before being deployed in a production environment

- security patches are downloaded from reliable sources and check for completeness

- security patches are not applied if they introduce additional vulnerabilities or instabilities that are more risky than the original reason for applying the patch

- reasons for not applying available security patches are documented

ÿ in cases where a security patch is not available, additional cybersecurity risk management measures are implemented and remaining risks are accepted

ÿ security patch management should be aligned with control procedures for change management and maintenance of network and information systems

5.6. ensure, if technically feasible, that a record is created of every report and activity on a critical network and information system in order to provide a forensic trail, and that tools and processes are used to monitor and record activities on the entity's network and information system in order to detect suspicious events that could constitute an incident and to take action to mitigate the potential impact of the incident. Log records must be kept for at least the last 90 days (not necessarily in the system that created them). As an exception, certain types of log records may be kept for a shorter period if the volume of such records represents a storage limit and if it is not possible to filter and/or compress such log records in order to retain key information and reduce the volume of records. When organizing the process of recording log records (scope and retention period), a risk assessment should be taken into account in order to enable the detection and investigation of incidents in accordance with the assessed risk scenarios. The entity must ensure that all systems have synchronized time so that log records can be correlated between different network and information systems. The following types of log records should be included as a minimum during the design of the network and information system:

ÿ metadata of outgoing and incoming network traffic

ÿ access to network and information systems, applications, network equipment and devices

ÿ creating, modifying and deleting user accounts and expanding rights

ÿ changes to backups

ÿ logs from security tools, such as an antivirus system, intrusion detection system or firewall

5.7. define and document the process of identifying and managing vulnerabilities in critical network and information systems that it independently develops. For this purpose, the entity must ensure a mechanism for identifying possible vulnerabilities in network and information systems that it independently develops. In accordance with its own risk assessment, mechanisms may include static code analysis tools (SAST), dynamic application analysis tools (DAST), third-party component verification (SCA), internal or external penetration tests, inclusion in reward programs (bug bounty) or similar. It is recommended to apply the principle of shifting security checks "to the left", i.e. to earlier phases of software development. If the entity does not apply the stated principles of shifting security checks "to the left", then adequate security testing must be carried out before releasing a new or changed network and information system into production.

CONDITION: Measure 5.7 is mandatory if the entity uses software solutions that it develops independently.

5.8. implement mechanisms for periodic or regular vulnerability checks of all network and information systems in order to timely detect the lack of application of security patches or incorrect system configuration. Entities are obliged, based on a risk assessment, to determine the need and frequency of this type of security testing (penetration tests, red teaming, purple teaming, etc.) in order to detect vulnerabilities in the implementation of the network and information system.

The results of security testing and vulnerability assessments should be prioritized, used to improve network and information system security, and monitored until resolved. Policies and procedures should be updated as necessary. The entity may limit this measure to critical software and hardware assets from measure 2.1.

5.9. ensure central storage of safety-relevant events by copying log records, continuously or at intervals not exceeding 24 hours, from the place where they were generated to a centralized system that enables storage and search and where are protected from unauthorized access and modification (if possible, the administrator of the source system should not be the administrator of this centralized system). Ensure that the central system has the ability to recognize anomalies and possible incidents and generate warnings about suspicious events. Monitoring of log records should take into account the importance of software and hardware assets and risk assessment - it is necessary to generate a larger, or it is permissible to generate a smaller number of different types of warnings about suspicious events, taking into account risk scenarios and assessed risks. The entity must check at pre-planned intervals whether the log records are recorded correctly by performing or simulating an action that should result in recording the appropriate log record. The entity must ensure that monitoring is implemented in a way that minimizes the occurrence of false positives and false negatives

5.10. ensure that controls are in place that prevent or detect the use of known or suspected malicious websites. The filter can be implemented by applying a list of prohibited categories or domain names, or by applying a list of allowed categories or domain names, depending on the subject's appetite for risk and business needs.

5.11. reduce the potential surface area of exposure of the entity to cyber-attacks:

- by identifying and limiting services that are publicly exposed/available via the Internet (for example, websites, e-mail, VPN entry points, monitoring consoles, RDP or SSH services for remote administration, SFTP, SMB and similar services for file exchange, etc.)

- by reducing the number of administrator and highly privileged user accounts

- by blocking access to publicly available services from the TOR network and known anonymizing VPN services

ÿ by limiting direct access to Internet servers, if possible.

Measures 5.1 to 5.11. apply in their entirety to the IT part of the entity's network and information systems. Points 5.1., 5.2., 5.3., 5.5., 5.6., 5.7., 5.8., 5.9., 5.10. and 5.11 above apply to OT systems, while point 5.4 above applies, depending on the risk assessment of implementing such a measure on OT systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure										
	5.1.	5.2.	5.3.	5.4.	5.5.	5.6. 5.7.		5.8.	5.9.	5.10.	5.11.
basic	AND	AND	AND	AND	AND	AND	C	AND	C	C	C
intermediate	AND	AND	AND	AND	AND	AND	B	AND	AND	AND	AND
advanced	AND	AND	AND	AND	AND	AND	B	AND	AND	AND	AND

6. Ensuring cyber security of the network

Objective: The objective of the measure is to ensure the integrity, confidentiality and availability of the entity's network resources.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

6.1. define and establish, in accordance with your network architecture and exposure to public networks, mandatory network protection measures and at the same time consider adequate measures such as the use of firewalls, virtual private networks (VPN), network access with constant application of the principle of zero trust ("everyone is untrustworthy"), security network protocols for wireless networks, separation of networks for different purposes, according to the criticality of data or the priority of individual network segments (for example, office network, surveillance network, production, manufacturing, guests, etc.)

6.2. ensure that mandatory network security measures ensure the secure transmission of critical data and the authorization and control of the use of networks and network-accessible resources. For example, the entity will ensure the use of secure versions of protocols such as HTTPS and sFTP, access to the network only for authorized individuals or devices (authorization may be based on the verified digital identity of the individual, the verified digital identity of the device, or both).

where otherwise it is not possible with the location of the connection if authorization of access to the location is carried out, for example a guarded office space or a data center)

6.3. conduct a comprehensive review of all defined network protection measures every year to ensure that they are still effective and relevant. This review includes an assessment of current cyber threats, vulnerabilities, and changes in the business environment that could affect the safeguards in place. Based on the results of the review, technical protection measures are updated to respond to new challenges and risks, ensuring constant compliance with best practices and requirements. All results and proposed changes must be documented and approved by the persons responsible for the implementation of the measures

6.4. implement mechanisms for monitoring outgoing and incoming network traffic in order to reduce the risk of cyberattacks and define methods for filtering unwanted network traffic in order to identify potential indicators of compromise.

This includes setting up appropriate tools for monitoring and analyzing network traffic that allow the identification and automatic blocking of potentially dangerous activities. The entity must also define and implement methods for filtering unwanted network traffic, such as the use of intrusion detection and prevention systems (IDS/

IPS) and other security solutions. All implemented filtering mechanisms and methods must be regularly reviewed and updated in order to maintain a high level of network security. This measure does not affect the prohibition of monitoring of electronic communications regulated by the law governing electronic communications

6.5. implement technical mechanisms for detecting network anomalies based either on deviations from typical network traffic or on deviations from internally defined rules.

Measures 6.1. to 6.5. apply in full to the IT part of the entity's network and information systems. The measures under points 6.1., 6.3. and 6.5 above apply in full to the entity's OT systems.

Point 6.2 above is also applicable to the OT part of the subject's network and information systems, depending on an additional assessment of the criticality of the subject's data in the OT system environment, while point 6.4 above is applicable, depending on an assessment of the possible negative impact of automatic blocking of potentially dangerous activities on the operational performance and security of the OT system.

Distribution of measure subsets by levels of management measures
cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure				
	6.1.	6.2. 6.3. 6.4.			6.5.
basic	AND	AAC			C
	AND	AND	AND	AND	C
intermediate advanced	AND	AND	AND	AND	AND

7. Control of physical and logical access to network and information systems

Objective: The objective of the measure is to establish a comprehensive system of policies and procedures to control physical and logical access to the subject's network and information systems, in order to prevent unauthorized access to program and circuit assets and subject data.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

7.1. develop, document, maintain and implement network and information system access control policies. Access control applies to all persons and external systems that access the network.

and information systems of the entity. The access control policy and rules should include the elaboration of access control for:

ÿ employees and staff of other entities that represent direct suppliers or service providers

ÿ processes within the network and information system of the entity, which are enabled to connect to another process outside the network and information system of the entity.

An entity does not have to document access control rules if it uses cloud computing services exclusively, but even in that case it must ensure the lifecycle management of the digital identities of all its users in accordance with measure 4.6.

7.2. ensure that owner roles are defined on applications that authorize the assignment of user rights and provide records of who authorized the assignment of rights. Access rights to network and information systems must be granted, modified, revoked, and documented in accordance with the entity's access control policy.

If access rights are defined through roles, each role must be assigned an owner. The owner of the role is responsible for granting rights. The entity must ensure records of role assignment approval in accordance with the logging and monitoring policy. The entity may decide to document or implement in its user rights assignment system a mapping of work roles to functional roles in individual network and information systems in order to manage digital identities more quickly and efficiently

7.3. carry out regular controls of user access rights. Access rights are reviewed and documented at planned intervals, at least once a year, and are adapted to organizational-business changes of the entity and are documented with appropriate monitoring of changes. The entity can limit this measure to critical program and structural assets from measure 2.1.

7.4. ensure supervision and control of access to critical network and information systems for privileged users. The entity must adopt and implement policies, i.e. rules, for the management of privileged accounts and system administrator accounts. The rules must include:

- creation of specific accounts that will be used exclusively for system administration activities, such as installation, configuration, management and maintenance

- individualization and limitation of administrator privileges as much as possible

ÿ use of privileged and administrator accounts exclusively for connecting to administration systems, and not for use in other business activities of the entity

- use of identification, strong authentication (examples of multi-factor authentication methods) and authorization procedures for privileged and administrator accounts

7.5. implement real-time, risk-based dynamic access control where possible and feasible using advanced tools

7.6. use advanced user behavior analysis of network and information systems (UEBA) that identifies unusual or suspicious user behavior, or cases in which there are irregularities that go beyond the framework of normal everyday patterns or usage.

Measures 7.1 to 7.6 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures
cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure					
	7.1.	7.2.	7.3.	7.4.	7.5.	7.6.
basic	AND	AND	AND	AND	C	C
	AND	AND	AND	AND	C	C
intermediate advanced	AND	AND	AND	AND	C	C

8. Supply chain security

Objective: The objective of the measure is to establish a clear and comprehensive policy for direct suppliers or service providers, especially key supply chains of ICT services, ICT systems or ICT products, in order to reduce identified risks and minimize vulnerabilities and optimize the entity's supply chain, which will result in more stable business and greater reliability of delivery of its products and services.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

8.1. develop, maintain, document and implement supply chain security policies that include minimum requirements for certain types of its direct suppliers and service providers, in particular those who supply entities with ICT services, ICT systems or ICT products, and a process for verifying the security of its direct suppliers and offered services that concern critical network and information systems. The entity must establish these policies for its direct suppliers and service providers, including the supply chain of ICT services, ICT systems or ICT products. The supply chain security policies contain roles, responsibilities and authorities including security aspects regarding the relationship between the entity and its direct suppliers or service providers. It is recommended that the entity defines policies for different suppliers if security aspects differ, for example different policies for suppliers of equipment and software in commercial offerings from policies for suppliers of custom software or cloud computing services (e.g. mandatory SSO) or providers of network and information system maintenance services

8.2. identify all its direct suppliers and service providers, including those in the supply chain of ICT services, ICT systems or ICT products, and assess the potential risks to the entity's network and information systems arising from these business relationships and, based on this, establish and maintain a register of direct suppliers and service providers that includes:

- contact points for each of them, and especially for those who have access to or manage critical software or circuit assets of the entity

ÿ a list of services, systems or products that the entity directly procures from identified direct suppliers and service providers

8.3. in business cooperation agreements or contracts for the procurement or provision of services (Service Level Agreement – SLA), define security requirements for its direct suppliers and service providers, which are aligned with the entity's cybersecurity policies.

Security requirements should include the following:

ÿ security clauses in contracts (for example, confidentiality provisions)

ÿ in the case of concluding contracts for the provision of managed services and managed security services, contracts for the provision of such services must be concluded exclusively with providers of such services that are categorized as key or important entities in accordance with the Act (verification of the categorization status of managed service providers and managed security service providers is carried out through the central state authority for cybersecurity)

ÿ provisions on the obligation of the direct supplier or service provider to notify the entity immediately upon learning of incidents that may affect the entity

ÿ provisions on the right to request a cybersecurity audit and/or the right to proof of a cybersecurity audit, or possession of appropriate equivalent certificates from the direct supplier

- provisions on the obligation to manage vulnerabilities, which includes the discovery of vulnerabilities and their elimination, as well as informing the subject about vulnerabilities that may affect the subject

ÿ provisions on possible subcontracting and safety requirements for subcontractors

ÿ provisions on the obligations of the direct supplier or service provider upon expiry or termination of the contractual relationship (for example, finding and removing/destroying/ disposing of data).

Security requirements may include the following:

ÿ provisions on skills and training required in relation to employees of the direct supplier or service provider

- provisions on certificates or other authorizations that are required are for employees of a direct supplier or service provider.

8.4. monitor, review, evaluate and repeat the process of verifying the security of key supply chains of ICT services, ICT systems or ICT products, at each new contracting or at least every two years or after an incident related to the service, system or product in question or after significant changes in security requirements or the state of cybersecurity.

Any deviations identified during the review and evaluation should be addressed through a risk assessment. The control of security requirements should cover all contractually defined security requirements.

8.5. define criteria and security requirements for the selection and conclusion of contracts with direct suppliers or service providers as well as criteria for evaluating and monitoring the security of individual suppliers and service providers, in particular those belonging to the key supply chain of ICT services, ICT systems or ICT products. The entity should strive to diversify its sources of supply in order to limit dependence on a single supplier or service provider and take into account the results of coordinated security risk assessments of key supply chains of ICT services, ICT systems or ICT products, carried out by the Cooperation Group together with the European Commission and ENISA, if available. When defining criteria and security requirements for the selection and conclusion of contracts, the entity is obliged to take into account:

ÿ the ability of suppliers and service providers to ensure the implementation of bu subject security requirements

ÿ own risks and the level of criticality of individual ICT services, ICT systems or ICT products it procures, including the risk tolerance of suppliers or service providers

8.6. develop incident response plans that include key suppliers and service providers, particularly those belonging to the key supply chain of ICT services, ICT systems or ICT products. The entity must develop incident response plans in accordance with documented procedures and within a reasonable timeframe. Incident response must also include the activities of key suppliers and service providers.

Measures 8.1 to 8.6 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure					
	8.1.	8.2.	8.3.	8.4.	8.5.	8.6.
basic	AND	AND	AND	AND	C	C
	AND	AND	AND	AND	AA	
intermediate advanced	AND	AND	AND	AND	AA	

9. Security in the development and maintenance of network and information systems system

Objective: The objective of the measure is to ensure that entities establish, document, implement and continuously monitor the configuration of their network and information systems, including the security settings of hardware and software assets, as well as the external services and networks they use.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

9.1. conduct an analysis of security requirements in the phases of technical specification development, design or procurement of network and information systems and define criteria for accepting solutions in accordance with defined security requirements

9.2. establish, document, implement and continuously monitor the configuration of its network and information systems, including security configuration settings for all hardware and software assets, as well as for all external services and networks used, throughout their lifecycle

9.3. prescribe procedures for managing changes in the framework of maintenance of network and information systems, which must include all used software and circuit support and changes to their configuration. The procedures are applied during release into the production environment, during all planned or unplanned changes to the program and circuit assets used or during any significant change in the configuration of network and information systems, as well as in the case of their development. Control procedures must be prescribed within the entity's cyber security policies, and all relevant employees of the entity should be familiar with them. In the case of urgent changes, it is necessary to document the results of the change, but also to provide an explanation as to why the regular change procedure could not be implemented and what the consequences of the delay would have been if the regular change procedure had been implemented. Testing that was not carried out due to urgent changes should be carried out later. Whenever possible, changes should be tested and validated before being rolled out to the production environment. Control procedures should include:

ÿ request for change

ÿ assessment of the risk posed by the change

ÿ criteria for categorization and prioritization of changes and associated requirements for the type and extent of testing to be performed and approvals to be obtained

ÿ requests for the implementation of a reversal procedure to return to the previous state

ÿ documentation on the change and approval of the change, including information on the responsible persons for each segment of the network and information system

9.4. develop, maintain and implement security rules in the processes of development and maintenance of network and information systems.
The entity must provide mechanisms for ensuring secure design (secure by design and by default) and zero-trust architecture, identification of possible vulnerabilities on network and information systems that it independently develops, integrates or implements, and define security requirements for development environments. Identification of potential vulnerabilities can be achieved during the early design phases by applying threat modeling methods, during development by various static (SAST) and dynamic (DAST) testing techniques, or after development is complete by various types of testing of the final product or system (e.g. penetration testing). It is recommended to apply the principle of shifting security checks to the left, i.e. to earlier phases of software development. The results of the security testing should be managed appropriately, as with all other risks

CONDITION: Measure 9.4. is binding for entities that independently develop or maintain network and information systems.

9.5. provide employees involved in the development of network and information systems with continuous training, define internal standards for the secure development of network and information systems, and conduct regular code security reviews. The measure can be implemented by applying some of the collaborative development methods (pair programming, two pairs of eyes when accepting code changes, test-driven development, etc.), using static code analysis tools (SAST), and the like, and the training of employees involved in the development of network and information systems must include at least:

ÿ analysis of security requirements in the phases of technical specification development and design or procurement of network and information systems

ÿ principles for designing secure systems and principles of secure programming, such as security-by-design, threat modeling, or zero-trust architecture

ÿ compliance with security requirements for development environments

ÿ use of security testing within the development lifecycle

CONDITION: Measure 9.5 is binding for entities that independently develop or maintain network and information systems.

9.6. integrate security tools and processes into development operations and practices (DevOps, DevSecOps), i.e. ensure security verification within the continuous integration and delivery (CI/CD) process. Entities must establish, document, implement and continuously monitor the configuration of their network and information systems, including security configuration settings of hardware and software assets, which includes application within the continuous integration and continuous delivery process methodology, and in accordance with the chosen practice.

Measures 9.1 to 9.6 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of measures					
	9.1.	9.2.	9.3.	9.4.	9.5.	9.6.
basic	AA		AC		C	C
	AA		AND	B	B	C
intermediate advanced	AA		AND	B	B	C

10. Cryptography

Objective: The objective of the measure is for entities, in accordance with their own business needs, to establish comprehensive cryptographic policies and procedures to ensure the protection of data in transit and at rest. The implementation of cryptographic policies should ensure the use of appropriate cryptographic techniques and algorithms, in accordance with best practices and regulatory requirements.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

10.1. develop, document, maintain and implement cryptography application rules in the entity, with the aim of ensuring the appropriate and effective use of cryptography to protect the availability, authenticity, integrity and confidentiality of critical data in accordance with the type of data and the results of the risk assessment

10.2. use encryption methods to protect critical data in transit. Cryptographic algorithms, padding methods, and key sizes for individual algorithms should be adapted to current good practices and must be proportionate to the risk and need to protect the subject

10.3. ensure secure cryptographic key management, which includes ensuring that cryptographic keys are protected from unauthorized access. The entity must define and document access rules for cryptographic key management, including methods for:

ÿ key generation for various cryptographic systems and applications

- issuing and obtaining certificates with public keys

ÿ distribution of keys to end users, including rules activation of received keys

ÿ key storage, including key access rules by authorized users

ÿ replacement or updating of keys, including rules on the method and time periods for key replacement

ÿ handling compromised keys

ÿ key revocation, including rules on how to withdraw or deactivate keys

ÿ recovery of keys that have been lost or damaged

ÿ secure storage or archiving of keys

ÿ destruction of keys

- recording and monitoring activities related to key management

ÿ determining the validity period of keys

10.4. implement encryption methods to protect critical data at rest. According to the criticality of the data, the subject will implement methods of protecting critical data at rest. The methods must include all media on which the data in question is stored at rest. Cryptographic algorithms, padding methods and key sizes for individual algorithms should be adapted to current good practices and must be proportional to the subject's estimated risk and the subject's need for protection

10.5. Conduct regular reviews and updates of cryptographic policies and procedures. Obligors are required to update cryptographic policies and procedures at planned intervals and in accordance with the latest developments in cryptography.

10.6. in accordance with the assessed risk, use quantum-resistant cryptography to protect against future threats in cases where this is possible.

Measures 10.1. to 10.6. apply to the entity's critical data from measure 2.3. and in accordance with the entity's risk assessment, regardless of whether the data is located on the IT or OT part of the entity's network and information systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure					
	10.1.	10.2.	10.3.	10.4.	10.5.	10.6.
basic	AND	AND	AND	AND	C	C
	AND	AND	AND	AND	AND	C
intermediate advanced	AND	AND	AND	AND	AND	C

11. Incident handling

Objective: The objective of the measure is to establish a comprehensive framework for determining roles, responsibilities and procedures that will enable the entity to effectively prevent, detect, analyze, contain and respond to incidents and recover from incidents.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

11.1. develop and document procedures for dealing with incidents, which includes defining roles, responsibilities and procedures for monitoring, preventing, detecting, analyzing, stopping and responding to incidents, recovering from incidents and recording and internally reporting incidents in clearly defined time frames

11.2. establish basic procedures for handling incidents- which the entity must provide at least the following:

ÿ establishing effective communication plans, including plans for classifying incidents according to national taxonomy, internal escalation and reporting of incidents. In doing so, the entity will, in accordance with the risk assessment, include in the communication plans rules for the use of multi-factor authentication or continuous authentication solutions, protected voice, video and text communications and secure communication systems in emergencies.

ÿ assigning incident detection and response roles to competent employees

ÿ rules for handling documentation that will be used or generated during incident handling, which may include incident response manuals, escalation charts, contact lists, and forms that need to be completed and submitted to the relevant authorities

ÿ introduction of a simple mechanism that allows employees of the entity and its direct suppliers and service providers to report suspicious events that could constitute an incident

ÿ it is necessary to assess the impact of each individual incident on the entity's business continuity and to appropriately establish an interface between incident handling and the entity's business continuity management

ÿ recording incidents

ÿ monitoring all elements necessary for identifying and monitoring significant incidents and timely notification of significant incidents to the competent CSIRT, in accordance with the prescribed obligations of the entity.

11.3. provide basic employee training for recognizing and reporting suspicious events and incidents, which must be repeated at least once a year for all employees. The implementation of the training must be documented. Training must be adapted to the business needs of the entity

11.4. develop and document detailed procedures for monitoring, analyzing and responding to incidents, taking into account a defined timeframe for internal incident reporting. The entity is required to define and document rules for triaging suspicious events, which determine the order in which such events will be assessed and processed.

events. In the triage process, when assessing a certain suspicious event, it is possible to assess that a certain suspicious event is likely to be a false positive event or that the possible impact of such an event is likely to be less than expected, on the basis of which the priority for further assessment and processing of that suspicious event can then be reduced, i.e. it can be moved on to assessing other suspicious events before the final processing and assessment of that event is completed. The entity is obliged to define procedures for stopping an incident, responding to an incident and recovering from an incident, in order to prevent the incident and its recurrence, as well as its spread and elimination of its consequences.
The entity is obliged to define procedures for notifying the competent CSIRT about significant incidents, as well as for reporting relevant internal and external users of its network and information systems, in accordance with the defined communication plan and the prescribed obligations of the entity.

11.5. conduct once a year exercises in dealing with simulated incidents for the purpose of checking the effectiveness of established procedures for monitoring, analyzing and responding to incidents. The subject is obliged to document the implementation of exercises in the same way as real incidents, with a clear note in the documentation that is created during the implementation of the exercise that it is not a real incident but an exercise. These can be red teaming exercises, table top simulation exercises and purple teaming/adversary emulation & detection engineering exercises

11.6. use specialized tools for automated incident detection and response (IDR/EDR/XDR/NDR). These tools should be adequately included and connected to other security controls. As the volume of suspicious events can be large, it is important that the entity does not find itself in a situation where, from a large volume of suspicious events, it fails to recognize key information indicating that a significant incident has occurred. It is more important for the entity to process and assess a smaller number of key suspicious events than to process and assess a larger number of all other suspicious events. Therefore, it is necessary that each suspicious event has an appropriate level of priority, based on which the triage process will determine the order in which suspicious events will be processed.

Measures 11.1 to 11.5 apply in full to both the IT and OT parts of the entity's network and information systems, while point 11.6 above is applicable, depending on the assessment of the possible negative impact of automated incident detection and response with regard to the operational performance and security of the OT system.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation: Subsets of measures

Level						
	11.1.	11.2.	11.3.	11.4.	11.5.	11.6.
basic	AND	AND	AND	AND	C	C
	AND	AND	AND	AND	AA	
intermediate advanced	AND	AND	AND	AND	AA	

12. Business continuity and cybercrisis management

Objective: The objective of the measure is to ensure the existence of pre-prepared plans for minimizing interruptions in business and ensuring the continuity of the entity's key business activities in cases of incidents and cyber crises.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

12.1. develop, maintain and implement business continuity and cybercrisis management policies, which will identify the entity's key business activities and the organizational and technical prerequisites for their implementation, as a basis for developing plans for a possible reduced scope of operations during incident recovery and a return to normal business operations within a defined timeframe and scope of operations acceptable to the entity

12.2. conduct an analysis of the impact of incidents on business (Business-ss Impact Analysis - BIA), which will identify key business functions and risk assessment as a prerequisite for the development of incident recovery plans. Based on the results of this analysis and risk assessment, the subject must establish at least:

ÿ Recovery Time Objectives (RTOs) to determine the maximum allowable time that can elapse for the recovery of business resources and functions after an interruption in the operation of individual segments of network and information systems

- time points of recovery (Recovery Point Objectives - RPOs) in order to determine how much data can be lost per individual business activity that is carried out using the network and information system, i.e. using ICT services and ICT processes that may be interrupted

- Service Delivery Objectives (SDOs) to determine the minimum level of performance that should be achieved to enable operations during the alternative mode of operation

ÿ RPO, RTO and SDO must be taken into account when determining backup and redundancy policies. Likewise, RPO, RTO, SDO must be taken into account when managing supply chain security, as well as security in the procurement, development and maintenance of network and information systems, including vulnerability remediation and their detection

ÿ list of key utilities required for normal operation
network and information systems

12.3. establish processes for cybercrisis management, i.e. for cases of large-scale cyber security incidents, while ensuring that cybercrisis management processes address at least:

- the roles and responsibilities of the entity's employees, in order to ensure that all employees are familiar with their roles in crisis situations, including specific steps that need to be followed

ÿ appropriate communication measures between the entity and relevant competent authorities in accordance with the National Cyber Crisis Management Program

ÿ maintaining the established level of cybersecurity of the entity in crisis situations through the implementation of appropriate measures, such as systems and processes for support and the establishment of possible additional capacities

- implementation of the process for management and use of information obtained from the competent CSIRT or other competent body related to incidents, vulnerabilities, cyber threats and necessary cyber security risk management measures

12.4. develop detailed disaster recovery plans (DRP) and business continuity plans (BCP). Based on the results of the risk assessment and business continuity plan, the entity's data backup and redundancy plan should be developed, maintained and documented, and must take into account at least:

ÿ recovery time

ÿ ensuring that backups or redundant systems are complete and correct, including configuration data and data stored in the cloud computing service environment

ÿ storage of (online and offline) backup copies and redundant systems in a secure location or locations, which are not on

on the same network as the primary system and are at a sufficient distance to avoid any damage from a disaster at the main location

- application of appropriate physical controls (such as access restriction) and logical controls (such as encryption) for backup copies, in accordance with the level of criticality of the data on these copies

ÿ restoring data from backups or activating switching to redundant systems, including the approval process

ÿ dependence on key utilities

ÿ a timeline of recovery activities related to the time schedule and interdependencies of individual recovery activities

12.5. conduct testing of business continuity plans at least once a year. Business continuity plans must be tested through exercises and revised periodically, following incidents, changes in operations or assessed risks. The testing of business continuity plans must be documented in order to unambiguously determine the necessary improvements observed during the testing. When testing a business continuity plan, the following must be tested:

ÿ roles and responsibilities

ÿ key contacts, i.e. contacts of employees with the necessary responsibilities, authorities and capabilities

ÿ internal and external communication channels

- conditions for activation and deactivation of the plan

ÿ sequence of procedures for recovery

- recovery plan for specific operations

ÿ required resources, including backups and redundancies

ÿ minimal recovery, and depending on plans, restart of activities (Restore) after temporary measures

ÿ connection with incident handling

ÿ network and information systems, such as hardware, software, services, data, etc. (such as redundant network devices, servers behind a load balancing system, RAID disk arrays, backup services, multiple data centers)

ÿ assets, including facilities, equipment and supplies

- use of alternative and redundant sources of power supply

12.6. conduct cyber crisis management exercises to test the entity's resilience to situations that cannot be predicted and planned for, taking into account:

- employee roles and responsibilities, to ensure that all employees are familiar with their roles in crisis situations, including specific steps to follow

ÿ appropriate communication measures between the entity and the relevant competent authorities

ÿ maintaining the established level of cybersecurity in crisis situations through the implementation of appropriate measures, such as support systems and processes and the establishment of additional capacity

CONDITION: Measure 12.6. is implemented as mandatory at the request of the competent authorities within the framework of the implementation of cyber crisis management exercises.

12.7. implement redundancy for critical network and information systems and critical data. When implementing, the entity must consider the options of investing in its own redundancy or engaging a third party to provide the necessary redundancy and document this. Redundancy should be considered in part or in full for:

ÿ network and information systems, such as hardware, software, services, data, etc. (such as redundant network devices, servers behind a load balancing system, RAID disk arrays, backup services, multiple data centers)

ÿ assets, including facilities, equipment and supplies

ÿ employees with the necessary responsibilities, authorities and capabilities

ÿ appropriate communication channels

ÿ key utilities

12.8. use redundant data centers in locations where the probability of the same geographic location threats occurring is lower.
The entity must conduct a risk assessment of the geographical location using available data (e.g. earthquake zones). The risk assessment must be documented. Based on the risk assessment, the selection and use of different data centers must be defined and implemented, taking into account positive legal regulations.
The entity can conduct an analysis to determine whether the cost of using a redundant data center outweighs the potential losses of not using it. In this case, the persons responsible for managing the measures can accept the risk in accordance with the risk management process.

Measures 12.1 to 12.8 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure							
	12.1.	12.2.	12.3.	12.4.	12.5.	12.6.	12.7.	12.8.
basic	A	A	A	A	C	B	C	C
	A	A	A	A	A	A	A	A
intermediate	A	A	A	A	A	B	A	A
advanced	A	A	A	A	A	B	A	A

13. Physical security

Objective: The objective is to establish measures to prevent and monitor unauthorized physical access to an entity's network and information systems, so that the entity can protect these systems from possible damage and disruption caused by physical threats.

The entity will implement the following sub-sets of measures within the framework of the implementation of this measure:

13.1. develop and implement a physical security policy in accordance with the risks within its ecosystem. The policy should, at a minimum, specify the scope of application, levels of protection for individual areas, methods of application, responsible persons and the frequency of checking the effectiveness of the measures. The policy, as well as changes to the policy, must be communicated to all employees and relevant legal entities with whom the entity has a business relationship

13.2. provide basic physical security measures such as appropriate physical barriers, locks, security cameras and access controls.
For defined security perimeters containing network and information systems and other related equipment, technical protection must be in place to ensure access to the premises depending on the entity's risk assessment, taking into account the potential criticality of the network and information system and the criticality of the software and hardware assets located in that area.

13.3. regularly review and update security protocols for physical locations. Security protocols to prevent unauthorized access should be established for critical network and information systems in order to reduce risk. Security protocols must reflect the criticality of the network and information systems to which they apply.

13.4. implement more advanced physical protection measures that ensure a clear record of access and can be used for subsequent digital forensics. The entity must implement more advanced physical protection measures in accordance with its risk assessment and in terms of enabling data exchange with other surveillance systems (records management system) in order to uniquely store access data and enable analysis during surveillance or an incident

13.5. in accordance with the entity's risk assessment, implement real-time surveillance of areas with critical software and hardware assets.

Measures 13.1 to 13.5 apply in their entirety to both the IT and OT parts of the entity's network and information systems.

Distribution of measure subsets by levels of management measures cyber security risks from Article 42 of this Regulation:

Level	Subsets of the measure				
	13.1.	13.2.	13.3.	13.4.	13.5.
basic	AND	AND	AND	C	C
	AND	AND	AND	AND	C
intermediate advanced	AND	AND	AND	AND	AND

ANNEX III.

SPECIAL PHYSICAL SECURITY MEASURES FOR ENTITIES FROM DIGITAL INFRASTRUCTURE SECTOR

Objective: The objective of these measures is to prevent and monitor the possibility of unauthorized physical access to the perimeter and facilities housing network and information systems that entities from the digital infrastructure sector from Annex I of the Act use in their business, as well as to prevent possible damage and disruption to their network and information systems caused by intentional, unintentional and natural physical threats.

Key and important entities from the digital infrastructure sector from Annex I of the Act are obliged to implement the following physical security measures features:

1. Develop a physical security plan that must include:

- physical security risk assessment as part of the risk assessment carried out by the entity within the framework of the implementation of the measure called "Risk Management" from point 3 of Annex II. of this Regulation

– determining the subject's premises that need to be protected and determining the level of physical security that needs to be ensured for each such space, taking into account the specifics of the space for housing network and information systems

– selection of physical security measures for the external perimeter, facilities and spaces where the entity's critical network and information systems are located

– list of access rights to facilities and areas referred to in indent 2 of this point and obligations and responsibilities of the entity's employees, security personnel, external associates and visitors

– a plan for conducting periodic physical security testing, taking into account that it must be conducted at least once a year as part of the risk assessment referred to in indent 1 of this point

– method of implementing regular maintenance of the physical security system things.

Additionally, in relation to each of the areas with a different level of required physical security, the physical security plan establishes the following physical security elements:

– access control of persons, access authorizations of employees, security personnel, external collaborators and visitors to a particular area

– equipment for implementing physical security measures that is installed in a particular space

– action plan for security personnel or external intervention teams in relation to a particular area.

2. Use multiple physical security measures at each location being protected. By introducing multiple physical security measures, it is necessary to ensure that they complement each other, whereby multiple systems for the same or similar purpose can be installed, all with the aim of reducing the likelihood of physical threats. The establishment of multiple measures is carried out by determining the location to be protected, determining the external perimeter, the perimeter of the facility and the perimeters of individual spaces within the facility with different levels of physical security. External physical security measures are applied to the external perimeter, they define the boundaries of the external space being protected and these measures must deter unauthorized access. Physical security measures applied within the protected space must ensure the identification of possible attempts at unauthorized access, which is simultaneously notified to security personnel and records are stored of all accesses to such spaces.

Physical security measures that are established closest to the areas with the entity's network and information systems must additionally slow down or prevent unauthorized access until security officers or intervention teams arrive at the location, but also ensure records of the presence of authorized persons in a particular area in case of investigation.

3. It is necessary to clearly physically separate the area that represents the external perimeter under the control of the entity from the public area or other area with which it borders. Clear warnings must be placed on the external perimeter about the prohibition of entry for unauthorized persons. The entity must ensure access through the external perimeter for vehicles and persons, while also determining the area for the delivery of equipment, as well as the area for the introduction of external associates and other visitors. The internal areas of the facility in which the entity has network and information systems must be appropriately divided into areas where external associates and other visitors can enter and areas that are exclusively for the use of employees or only for a certain category of employees. The entry of vehicles, external associates and other visitors must be covered by appropriate control measures and be in accordance with the entity's rules on the possibility of bringing technical equipment of external associates and visitors or private technical equipment of the entity's employees into individual areas with different levels of physical security.

4. Implement access control using mechanical, electronic or procedural means, or a combination of these means. Mechanical access control should be based on the use of security locks and security keys on the doors of protected areas. Electronic access control should be based on the use of an automatic access control system that uses some type of digital cards and PINs or biometrics. Procedural access control should be based on the establishment of checkpoints with security officers located at convenient locations at the approach to the external perimeter or entrance to the subject's facility. Access control should be implemented for all areas of the subject by direct inspection of security passes by security officers or by another method of unambiguous identification of the person (automatic access control system), with an appropriate method of keeping records of access. Detection of unauthorized access should be implemented to enable an effective and timely response to an attempted

unauthorized access within the external perimeter or within the subject's facilities, as well as for the purpose of subsequent analysis in order to identify the perpetrators of such actions. Detection of unauthorized access should be carried out in various ways, depending on the established level of physical security of a particular area. Detection of unauthorized access should be carried out using security personnel, external intervention teams or using various electronic systems, or a combination of these measures.

5. Appropriately protect the storage of the entity's critical data, which includes data in physical and electronic form, taking into account that the storage of data related to the provision of services from the digital infrastructure sector from Annex I to the Act generally includes data in electronic form. Physical protection of critical data in physical form must be carried out by using appropriate security containers located in premises with an appropriate level of physical security measures or by using spaces for open storage of critical data, without security containers, but with an appropriate level of physical security measures established for such premises. Physical protection of critical data in electronic form must be carried out by physically protecting the premises in which network and information systems are located that entities from the digital infrastructure sector from Annex I to the Act use in their business, and in particular in which sensitive client computer equipment is located. The entity is obliged to establish rules for access by persons for all premises in which critical data is stored, rules for bringing in technical equipment, as well as rules for bringing in and using employees' private technical equipment in individual premises with different physical security requirements.

6. The premises where servers and other equipment for managing the network and information systems of the entity are located must be organized as specially supervised premises, to which only persons responsible for the security and administration of such systems, or maintenance personnel, have the right to access, but only when constantly accompanied by persons responsible for the security of the entity and the administration of such systems. Access to such premises must be protected by an appropriate access control system and systems for detecting unauthorized access. Client computer equipment that is sensitive to unauthorized physical access shall be placed in premises that have an appropriate level of physical security measures and must be used in such premises, or under the control of a competent employee of the entity. For persons responsible for managing the measures, as well as persons responsible for the security and administration of the network and information systems of the entity, the entity is obliged to obtain information on the non-criminal record of these persons, or an appropriate certificate of non-criminal record, and to update the relevant information periodically, at least every five years.

ANNEX IV.

DECLARATION OF CONFORMITY
OF ESTABLISHED MANAGEMENT MEASURES
CYBERNETIC SECURITY RISKS

SUBJECT INFORMATION	
NAME	
ADDRESS	
SECTOR SUBSECTOR TYPE OF SUBJECT	
SECTOR MAIN BUSINESS ACTIVITY	

CYBER SECURITY SELF-ASSESSMENT	
DETERMINED LEVEL OF CYBER SECURITY SNOWLEDGE RISKS	
LEVEL OF CYBER MANAGEMENT MEASURES SECURITY RISKS IDENTIFIED BINDING	
TOTAL SCORE OF THE DEGREE OF HARMONIZATION OF MEASURES CYBERNETIC SECURITY MANAGEMENT RISKS	
TOTAL LEVEL UP TREND POINTS MATURITY	
LIST OF DOCUMENTATION	
NAME, SURNAME AND SIGNATURE OF THE PERSON WHO CARRIED OUT SELF-ASSESSMENT PROCEDURE	

DECLARATION OF CONFORMITY	
The results of the cyber security self-assessment for the subject show that cyber security risk management measures have been established in accordance with the cyber security risk management measures prescribed by the Cyber Security Act and the Cyber Security Regulation.	
NAME, SURNAME AND SIGNATURE OF THE PERSON RESPONSIBLE FOR MANAGING CYBER SECURITY RISKS MANAGEMENT MEASURES	

2218

Pursuant to Article 30, paragraph 2 of the Act on the Government of the Republic of Croatia (Official Gazette, Nos. 150/11, 119/14, 93/16, 116/18, 80/22 and 78/24), the Government of the Republic of Croatia, at its session held on 21 November 2024, adopted

REGULATION

ABOUT RATIONALIZATION MEASURES TO ACCELERATE IMPLEMENTATION OF THE TRANS-EUROPEAN TRANSPORT NETWORK (TEN-T)

Article 1.

This Regulation regulates the permitting procedures necessary for approving the implementation of:

a) projects that are part of previously identified sections of the core network, as set out in the Annex to this Regulation and which form an integral part thereof

b) other projects on core network corridors, as determined on the basis of Article 11(1) of Regulation (EU) 2024/1679 of the European Parliament and of the Council of 13 June 2024 on Union guidelines for the development of the trans-European transport network, amending Regulation (EU) 2021/1153 and Regulation (EU) No 913/2010 and repealing Regulation (EU) No 1315/2013 (OJ L 2024/1679, 28. 6. 2024) (hereinafter: Regulation (EU) 2024/1679), the total cost of which exceeds EUR 300,000,000.00, with the exception of projects relating exclusively to telematics applications, new technologies and innovations within the meaning of Articles 43 and 45 of Regulation (EU) 2024/1679.

Article 2.

This Regulation transposes Directive (EU) 2021/1187 of the European Parliament and of the Council of 7 July into Croatian legislation.