Machine Translated by Google

The Network and Information Systems Security (Amendment) Law of 2025 is issued by publication in the Official Gazette of the Republic of Cyprus in accordance with Article 52 of the Constitution.

Number 60(I) of 2025

LAW AMENDING THE NETWORK AND INFORMATION SYSTEMS SECURITY LAW OF 2020

The House of Representatives votes as follows:

Summary title. 89(I) of 2020.

1. This Law shall be cited as the Network and Information Systems Security (Amendment) Law of 2025 and shall be read together with the Network and Information Systems Security Law of 2020 (hereinafter referred to as "the principal law") and the principal law and this Law shall be cited together as the Network and Information Systems Security Laws of 2020 and 2025.

Amendment of the basic law with the replacement of the preamble.

2. The preamble to the basic law is replaced by the following preamble:

"Preamble.

(a) For the purposes of harmonization with the European Union act on title:

Official Gazette of the EU: L 333, 27.12.2022, p. 80.

"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 910/20214 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS Directive 2)"; and

(b) for purposes of partial harmonisation with the European Union act titled:

Official Her newspaper EU: L153, 22.5.2014, p. 62.

"Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC".».

Amendment of article 2 the basic law.

3. Article 2 of the basic law is amended as follows:

(a) By deleting subsection (1);

(b) by replacing subsection (2) with the following subsection:

"2(a) This Law shall apply without prejudice to the responsibility of the Republic for the safeguarding of national security and its sovereign right to safeguard other essential functions of the Republic, including the safeguarding of its territorial integrity and the maintenance of public order.

(b) Subject to the provisions of subsection (4), this Law shall not apply to public administration entities which carry out their activities in the fields of national security, public order, defence or law enforcement, including the prevention, investigation and prosecution of criminal offences.";

(c) by adding in subsection (3), immediately after the phrase "subject to" (first line), of the following sentence:

Official Journal of the EU: L119,

"Regulation (EU) 2016/679 on the Regulation of Electronic Communications and Postal Services"

Machine Translated by Google

4.5.2016,
p. 1.
112(I) of 2004
84(I) of 2005
149(I) of 2005
67(I) of 2006
113(I) of 2007
134(I) of 2007
46(I) of 2008
103(I) of 2009
94(I) of 2011
51(I) of 2012
160(I) of 2013
77(I) of 2014
104(I) of 2016
112(I) of 2016
76(I) of 2017
90(I) of 2020
23(I) of 2022.
24(I) of 2022.

"Law, the Regulation of Electronic Communications Law,"; and

(d) by adding, immediately after subsection (3), the following new subsections:

"(4)(a) The Authority, pursuant to the provisions of subsection (7) of section 27, may exempt specific entities which carry out activities in the fields of national security, public order, defence or law enforcement, including activities related to the prevention, investigation and prosecution of criminal offences or activities which provide services exclusively to the public administration bodies referred to in paragraph (b) of subsection (2) of section 2, from the obligations set out in section 35 or 35B of this Law in relation to such activities or services.

(b) In such cases, the supervisory and enforcement measures referred to in this Law shall not apply in relation to the specific activities or services and in the event that the entities carry out activities or provide services exclusively of the type referred to in this paragraph, the Authority may also decide to exempt such entities from the obligations set out in articles 27 and 37A of this Law.

(5) This Law does not apply to the security of information networks and systems, as well as to the infrastructure and facilities of the Cyprus Intelligence Service.".

Amendment of the basic law with the addition of the new article 2A.

4. The basic law is amended by adding, immediately after article 2, the following new article:

"Scope of application.
Official Gazette of the EU: L124, 20.5.2003, p. 36.
Appendix I.
Annex II.

2A.-(1)(a) This Law shall apply to public or private entities the type of which is referred to in Annex I or II, which, pursuant to Article 2 of the Annex to Recommendation 2003/361/EC, are classified as medium-sized enterprises or exceed the thresholds for medium-sized enterprises referred to in that Article and which provide their services or carry out their activities within the Union.

(b) Paragraph 4 of Article 3 of the Annex to Recommendation 2003/361/EC shall not apply for the purposes of this Law.

(2) This Law also applies to the type of entities listed in Annex I or II, regardless of their size, provided that-

Annex I.
Annex II.

Machine Translated by Google

(a) the services are provided by-

(i) providers of public electronic communications networks or publicly available electronic communications services;

(ii) trust service providers; and

(iii) top-level domain name registries (TLD registry) and domain name system service providers (domain name service provider) DNS);

(b) the entity is the sole provider in the Republic of a service that is essential for the maintenance of critical social or economic activities;

(c) the disruption of the service provided by the entity could have a significant impact on public security, public order or public health;

(d) the disruption of the service provided by the entity could cause significant systemic risk, in particular for sectors in which such disruption could have a cross-border impact;

(e) the entity is critical due to its particular importance at national or regional level for the specific sector or type of service or for other interdependent sectors in the Republic; and

(f) the entity is a public administration body;

(i) the central government, as defined in this Law;

(ii) the broader public sector, which, following a risk assessment, provides services whose disruption could have a significant impact on critical social or economic activities.

(3) Regardless of the size of the entities, this Law applies to entities that are designated as critical entities by the competent authority for the resilience of critical entities.

(4) Regardless of the size of the entities, this Law applies to entities that provide domain name registration services.

(5) Subject to the provisions of subsection (7) of article 27, this Law applies to public administration entities at local level and may be applied to educational institutions, in particular when they carry out critical research activities.

(6) The provisions of paragraph (b) of subsection (2) of article 2 and the provisions of subsection (4) of article 2 shall not apply in a case in which an entity acts as a trust service provider.

(7) The obligations provided for in this Law do not include the provision of information, the disclosure of which is incompatible with the essential interests of national security, public order or defence of the Republic.

(8) The entities and the Authority shall process personal data to the extent necessary for the purposes of this Law and in accordance with Regulation (EU) No.

Machine Translated by Google

2016/679, and in particular this processing is based on Article 6 of the said Regulation:

It is understood that the processing of personal data under this Law by providers of public electronic communications networks or providers of publicly available electronic communications services is carried out in accordance with Regulation (EU) 2016/679 on data protection, the Law on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and with regard to the protection of privacy, the Law on the Regulation of Electronic Communications and Postal Services and the Law on the Regulation of Electronic Communications.

125(I) of 2018
26(I) of 2022.

(9) Where sectoral Union legal acts require key or significant entities to adopt cybersecurity risk management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Law, the relevant provisions of this Law, including the provisions on supervision and enforcement provided for in Articles 36, 36A and 36B, shall not apply to those entities and where sectoral Union legal acts do not cover all entities in a specific area falling within the scope of this Law, the relevant provisions of this Law shall continue to apply to entities not covered by those sectoral Union legal acts.

(10) The requirements referred to in subsection (9) shall be deemed to be equivalent in effect to the obligations set out in this Law in the event that-

(a) the risk management measures in the field of cybersecurity are at least equivalent in effect to those measures provided for in paragraphs (1) and (2) of Article 35; or

(b) the sectoral Union legal act provides for immediate access, where appropriate automatic and direct, to incident notifications from CSIRTs, competent authorities or single points of contact under the provisions of this Law and whether the requirements for the notification of significant incidents are at least equivalent in effect to those requirements laid down in paragraphs (1) to (6) of Article 35B.'.

Amendment of article 3 the basic law.

5. Article 3 of the basic law is amended as follows:

(a) By adding, in subsection (1), in the appropriate alphabetical order, the following: following new terms and their definitions:

"information and communication technology process" or "ICT process" of Regulation (EU) 2019/881;

"public electronic communications network" has the meaning assigned to this term in article 5 of the Regulation of Electronic Communications Law;

"network" means the network of national coordination centres;

"content distribution network" means the network of geographically distributed servers which aims to ensure high availability and accessibility or rapid delivery of digital content

Machine Translated by Google

content and digital services to internet users on behalf of content and service providers;

“CSIRT Network” means the network established and operating pursuant to the provisions of Article 15 of Directive (EU) 2022/2555;

“qualified trust service” has the meaning assigned to that term in point (17) of Article 3 of Regulation (EU) No 910/2014;

Official Her newspaper EU: L257, 28.8.2014, p. 73.

“qualified trust service provider” has the meaning assigned to that term in point (20) of Article 3 of Regulation (EU) No 910/2014;

"representative" means a natural or legal person established either in the Republic or in other Member States who has been expressly designated to act on behalf of a DNS service provider, TLD registry, domain name registration service provider, cloud computing service provider, data center service provider, content distribution network provider, managed services provider, managed security services provider, online marketplace provider, online search engine or social networking service platform provider who is not established in the Republic or in another Member State, to whom the Authority or the national

CSIRT instead of the entity itself with regard to the obligations of that entity under this Law;

"single point of contact" has the meaning assigned to this term under the provisions of paragraph (c) of article 17 of this Law;

“EU-CyCLONe” means the European Network of Liaison Organisations for Cyber Crises;

"vulnerability" means the weakness, sensitivity or defect of ICT products or ICT services that could be exploited by a cyber threat;

“research activity” means the conduct of applied research or experimental development, as provided for in the Frascati Manual 2015 of the Organization for Economic Cooperation and Development entitled “Guidelines for the collection and reporting of data on research and experimental development, with a view to exploiting their results for commercial purposes, such as the manufacture or development of a product or process or the provision of a service or the marketing thereof”;

Annex II.

“research organisation” means the type of entity listed in Annex II which has as its primary objective the conduct of applied research or experimental development with a view to exploiting the results of such research for commercial purposes and does not include an educational institution;

“wider public sector” means independent services not included in the budget of the Republic, legal persons under public law and public law entities that are not part of the central government;

"day" means a calendar day, unless otherwise specified in this Law;

Official Journal of the EU: L151, 17.4.2019, p. 15.

“Regulation (EU) 2019/881” means Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the “European Union Agency for Cybersecurity”) and on cybersecurity certification in the information and communications technology sector and repealing

Machine Translated by Google

Regulation (EU) No 526/2013 (Cybersecurity Act), as amended or replaced from time to time;

Official Her newspaper EU: L333, 27.12.2022, p.114.

“Regulation (EU) 2022/2554” means Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, as amended or replaced from time to time;

“class of radio equipment” means the class which identifies specific categories of radio equipment which are considered similar under the provisions of this Law and those radio communications for which the radio equipment is designed;

"state body" or "central government" means the Ministries, Deputy Ministries, their departments, their services, their directorates, the bodies of constitutional powers and services, the independent services and the basic and/or important entities included in the budget of the Republic;

to the

“cybersecurity” has the meaning assigned to this term in point (1) of Article 2 of Regulation (EU) 2019/881;

“cyber threat” has the meaning assigned to that term in point (8) of Article 2 of Regulation (EU) 2019/881;

75(I) of 2016 14(I) of 2023.

“Cyprus Intelligence Service” means the independent authority established under the provisions of the Cyprus Intelligence Service (CIS) Law;

"top-level domain name registry" or "TLD registry"
(Top-level domain)' or 'TLD registry' means an entity to which a specific TLD has been assigned and which is responsible for the administration of the TLD, including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files to name servers, regardless of whether any of these acts are performed by the entity itself or outsourced, but excluding cases in which TLD names are used by a registry solely for its own use;

Official Her newspaper EU: L333, 27.12.2022, p.80.

“Directive (EU) 2022/2555” means 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 (NIS Directive 2), as amended or replaced from time to time;

Official Her newspaper EU: L153, 22.5.2014, p. 62.

“Directive 2014/53/EU” means Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC”, as amended or replaced from time to time;

“public administration entity” means an entity, not including the judiciary, the House of Representatives or the Central Bank of Cyprus, which meets the following criteria:

(a) It has been established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) has legal personality or is legally entitled to act on behalf of another entity with legal personality;

(c) is financed for the most part by the central government or other public law bodies, is subject to control

Machine Translated by Google

managed by those authorities or bodies or has an administrative, management or supervisory board, more than half of whose members are appointed by the State, the wider public sector or other bodies governed by public law; and

(d) has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;

"domain name registration service provider" means the registrar or an agent acting on behalf of registrars, such as a personal data registration service provider or an agent or reseller;

"entity" means a natural or legal person established and recognised as such under the national law of its place of establishment, which may, acting on its own behalf, exercise rights and be subject to obligations;

“Cooperation Group” means the Cooperation Group established in accordance with Article 14 of Directive (EU) 2022/2555;

‘managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of products, networks, infrastructure, ICT applications or any other network and information systems, through a subscription or active management performed either at the customers’ premises or remotely;

“person” means a key and/or significant entity, and any other legal or natural persons or organizations that the Authority from time to time deems to be a person for the purposes of this Law, based on its powers arising from this Law;

"near-miss" means an incident that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or existing processed data or services offered or accessible through network and information systems, but which was prevented or not successfully implemented;

"provider" means a person who provides or is authorised to provide an electronic communications network and/or services and/or related facilities to the public;

"managed security services provider" means a provider
managed services that performs or provides support for activities related to cybersecurity risk management;

“trust service provider” means a trust service provider as defined in point 19 of Article 3 of Regulation (EU) No 910/2014;

"DNS service provider" means an entity that provides:

(a) publicly available recursive domain name resolution services for internet end-users; or

(b) valid domain name resolution services for use by third parties, with the exception of root name servers;

"incident" means any event that compromises the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed or of services offered or accessible through network and information systems;

Machine Translated by Google

“large-scale cybersecurity incident” means an incident that causes a disruption that exceeds the capacity of the Republic or another Member State to respond to it or that has a significant impact on at least two Member States;

‘social networking service platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular through conversations, posts, videos and recommendations;

“ICT product” has the meaning assigned to that term in point (12) of Article 2 of Regulation (EU) 2019/881;

"radio equipment" means an electrical or electronic product that intentionally emits and/or receives radio waves for radiocommunication and/or radiodetermination purposes or an electrical or electronic product that must be supplemented with a component, such as an antenna, in order to intentionally emit and/or receive radio waves for radiocommunication and/or radiodetermination purposes;

‘significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be considered to have the potential to seriously affect the network and information systems of an entity or the users of the entity’s services, causing significant material or non-material damage;

“Recommendation 2003/361/EC” means the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;

“ICT” means information and communications technology;

“technical specification” has the meaning assigned to that term in point (4) of Article 2 of Regulation (EU) No 1025/2012;

"trust service" has the meaning assigned to this term in Article 3(16) of Regulation (EU) No. 910/2014;

"electronic communications service" means an electronic communications service, as defined in article 2 of the Regulation of Electronic Communications Law;

“ICT service” has the meaning assigned to that term in point (13) of Article 2 of Regulation (EU) 2019/881;

‘cloud computing service’ means a digital service that enables on-demand management and widespread remote access to a scalable and elastic pool of shared computing resources, including when those resources are distributed across multiple locations;

"incident management" means any action and process aimed at preventing, detecting, analysing and containing or responding to and recovering from an incident;

"data center service" means the service comprising structures or groups of structures, which are intended for the central hosting, interconnection and operation of information technology (IT) equipment and networks and provide data storage, processing and transmission services, as well as all power distribution and environmental control facilities and infrastructure;

(b) by deleting the following terms and their definitions:

(i) "representative"·

(ii) "critical infrastructure";

Machine Translated by Google

(iii) "Directive 2016/1148";

(iv) "critical information infrastructures";

(v) “top-level domain name registry”;

(vi) “digital service provider”;

(vii) “specification”;

(viii) “cloud computing service”; and

(ix) "event handling";

(c) by replacing the term "network and information systems security" and its definition with the following new term and definition:

“security of network and information systems” means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible through those network and information systems;”;

(d) by replacing the definition of the term ““Office” or “OCECPR”” with the following new definition:

““Office” or “OCECPR” means the Office of the Communications Commissioner established under the provisions of the Regulation of Electronic Communications and Postal Services Law;”;

(e) by replacing the term “network and information system” with the following new term “network and information system”;

(f) by replacing the term "national strategy for the security of networks and information systems and cybersecurity" and its definition with the following new term and definition:

““national cybersecurity strategy” means the coherent framework of the Republic which provides strategic objectives and priorities in the field of cybersecurity and governance for their achievement in the Republic;”;

(g) by replacing the definition of the term “online marketplace” with the following:
following definition:

“‘online marketplace’ means a service that uses software, including a website, part of a website or an application, operated by a trader or on behalf of the trader, and that allows consumers to conclude distance contracts with other traders or consumers using software, including a website, part of a website or an application, operated by a trader or on behalf of the trader;”;

(h) by replacing the definition of the term “online search engine” with the following new definition:

““online search engine” has the meaning assigned to that term in point (5) of Article 2 of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fair treatment and transparency for business users of online intermediation services;”;

Official
Her newspaper
EU: L186,
11.7.2019,
p. 57.

Machine Translated by Google

(i) by replacing the definition of the term “risk” with the following new definition:
definition:

““risk” means the possibility of loss or disruption caused by an event and is expressed as a combination of the magnitude of that loss or disruption and the probability of that event occurring;”;

(j) by replacing the definition of the term “Internet Exchange Point” or “IXP” with the following new definition:

"Internet Exchange Point" or
“IXP” means a network facility that allows the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of Internet traffic, which provides interconnection only for autonomous systems and which neither requires Internet traffic passing between a pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise affects such traffic;”;

(k) by replacing the definition of the term "domain name system" (Domain Name System)” or “DNS” with the following new definition:

“Domain Name System” or “DNS” means the hierarchical distributed naming system that allows the identification of Internet services and resources, allowing end-user devices to use Internet routing and connectivity services to access those services and resources;”;

(l) by replacing the definition of the term "operator of essential services" services" with the following new definition:

““operator of essential services” means the public or private entity of a type referred to in a Decision issued by the Authority;”; and

(m) by adding to the definition of the term "digital service", immediately after the phrase "paragraph 1", (first line), the phrase "item b)".

Amendment of article 6 the basic law.

6. Article 6 of the basic law is amended as follows:

(a) By replacing subsection (4) with the following subsection:

“(4) The Authority continues to be staffed and administered pursuant to the provisions of the Regulation of Electronic Communications and Postal Services Law and pursuant to the provisions of this Law and the Decisions and Regulations issued pursuant thereto.”; and

(b) by adding, immediately after subsection (9), the following new subsection:

"(10) The Commissioner has the authority to advise the Deputy Minister on matters relating to the security of network and information systems, digital security and cybersecurity in the Republic.".

Amendment of article 7 the basic law.

7. Article 7 of the basic law is amended by replacing paragraph (b) with the following new paragraph:

"(b) accepts the provision of grants, for the purposes of implementing the provisions of this Law, from the Republic, the European Union, an international organization or a company or organization, provided that the organization is not a key or significant entity that has a financial or other interest, direct or indirect, with the Authority and is not, in any case, involved in any such key or significant entity,".

Machine Translated by Google

Amendment the basic law with the deletion of article 9.

8. The basic law is amended by deleting article 9.

Amendment of article 11 the basic law.

9. Article 11 of the basic law is amended by replacing in paragraph (a) of subsection (1) the phrase “operators of essential services and critical information infrastructure operators, digital service providers and providers of electronic communications networks and/or services” (first to third lines), with the phrase “the essential and important entities”.

Amendment of article 15 the basic law.

10. Article 15 of the basic law is amended as follows:

(a) By replacing subsection (1) with the following subsection:

“(1) In exercising the responsibilities and powers of the Authority, pursuant to the provisions of this Law and in performing its duties, the Authority shall act in a manner that promotes the maintenance of the integrity and security of electronic communications networks, the achievement of a level of security of network and information systems, including the protection of entities falling under the authority of the Authority.”;

(b) by deleting subsection (2); and

(c) by replacing subsection (3) with the following subsection:

"(3) With regard to matters falling within the fields of defence, national security, public security, public order, foreign policy of the Republic as well as in the fields of the mission of the Cyprus Intelligence Service, as defined in the Cyprus Intelligence Service (CIS) Law, the Authority is obliged to comply with the instructions and/or Decisions of the Council of Ministers when exercising its powers under the provisions of this Law.".

Amendment of article 16 the basic law.

11. Article 16 of the basic law is amended by replacing subsection (2) with the following subsection:

"(2) The Deputy Minister shall determine and/or review the general policy framework in relation to digital security.".

Amendment of article 17 the basic law.

12. Article 17 of the basic law is amended as follows:

(a) By deleting paragraph (a);

(b) by replacing in paragraph (c) the word "centre" (first and second line), with the word "point";

(c) by amending paragraph (d) as follows:

(i) by replacing the word "center" (first line), with the word "point"; and

(ii) by replacing the phrase “and the CSIRT Network” (third line), with the phrase “the CSIRT Network and EU-CyCLONE,”;

Machine Translated by Google

(d) by replacing paragraph (e) with the following paragraph:

"(e) consult and cooperate with the competent law enforcement authorities, the Cyprus Intelligence Service, the Commissioner for Personal Data Protection, the Department of Civil Aviation, the Department of Electronic Communications, the competent authorities of the Republic designated for the implementation of Regulation (EU) 2022/2554, OCECPR and the competent authority of the Republic for the resilience of critical entities, as well as with the competent authorities designated under other sectoral legal acts of the Union;";

(e) by amending paragraph (f) as follows:

(i) By replacing the word "center" (first line), with the word "point"; and

(ii) by replacing the phrase "subsections (3) and (5) of article 35 and the provisions of subsections (3) and (6) of article 37" (sixth to eighth lines), with the phrase "subsections (4) and (6) of article 35B";

(f) by amending paragraph (g) as follows:

(i) By adding immediately after the word "ensures" (first line), the phrase "through the Council of Ministers," and

(ii) by replacing the phrase "paragraph (a) of subsection (2) of article 31" (third and fourth lines), with the phrase "subsection (3) of article 31 and the provisions of subsection (3) of article 31A";

(g) by adding in paragraph (i), immediately after the phrase "development of the national CSIRT" (second and third lines), the phrase ", if the Authority deems it necessary,";

(h) by replacing in paragraph (j), the word "events" (first line), with the word "incidents";

(i) by deleting paragraph (k);

(j) by deleting in paragraph (l) the phrase "the government CSIRT, the academic CSIRT or" (first line);

(k) by adding in paragraph (m), immediately after the phrase "at national level" (second line), the phrase "in accordance with the provisions of this Law,";

(l) by replacing paragraph (n) with the following paragraph:

"(n) designates, by its Decision, the basic and significant entities established in the Republic for each sector and sub-sector referred to in Annex I or II of this Law as well as the entities providing domain name registration services in the Republic,";

Annex I.
Annex II.

(m) by replacing paragraph (o) with the following paragraph:

"(o) review and, where appropriate, update the list of identified key and significant entities and entities providing domain name registration services on a regular basis and at least every two years,";

(n) by replacing in paragraph (q) the phrase "operators of essential services and/or critical information infrastructure operators" (first and second lines), with the phrase "essential and/or important entities";

Machine Translated by Google

(o) by amending paragraph (o) as follows:

(i) By replacing the phrase “operators of essential services and/or critical information infrastructure operators” (first and second lines), with the phrase “essential and/or important entities” and

(ii) by adding, immediately after the phrase “appropriate and proportionate technical” (second and third lines), the word “operational”;

(p) by replacing paragraph (s) with the following paragraph:

“(s) ensures that key and/or significant entities take appropriate measures for a holistic approach to risk aimed at protecting network and information systems and the physical environment of those systems from incidents,”;

(q) by replacing paragraph (k) with the following paragraph:

“(k) ensures that key and/or significant entities promptly notify the Authority of any incident that has a significant impact on the provision of their services, as referred to in subsection (3) of article 35B (significant incident),”;

(r) by deleting paragraphs (ka), (kb), (kc) and (kd);

(s) by replacing in paragraph (kst) the phrase "of article 43" (first line), with the phrase "of articles 43 and 43A";

(k) by replacing paragraph (k) with the following paragraph:

“(ii) requests, in the context of its specific activities, the provision, from the key and/or significant entities and/or entities providing domain name registration services, of any relevant technical, financial and other information, including logs, for a period of at least six (6) months, as well as information for public order and national security purposes, in compliance with the principle of proportionality,”;

(ka) by deleting in paragraph (la) the phrase "provisions of subsection (13) of article 37 and" (second and third lines);

(kv) by replacing the comma at the end of paragraph (ld) with a colon and adding, immediately afterwards, the following reservations:

"It is understood that the Authority may conclude memoranda of understanding with national computer incident response teams of a third country and, in this context, the Authority shall facilitate the effective, efficient and secure exchange of information with such national computer incident response teams of a third country, using relevant information exchange protocols, including the Traffic Light Protocol."

Light Protocol – TLP):

It is further understood that the Authority may exchange relevant information with national teams responding to security incidents in third-country computers, including personal data pursuant to the provisions of the Law on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data and Regulation (EU) 2016/679,”;

(k) by amending paragraph (k) as follows:

(i) By replacing the phrase “as operators of essential services or operators of critical information infrastructures” (seventh to ninth lines), with the phrase “essential or important entities”; and

Machine Translated by Google

(ii) by replacing the full stop (ninth line) with a comma;

(kd) by adding, immediately after paragraph (le), the following new paragraphs:

"(lst) issues, within the framework of the effective exercise of its responsibilities and powers, Decisions for the implementation of Union Regulations, the harmonisation with Union Directive, Decision, Executive Regulation, delegated Regulation, Recommendation and any other relevant act of the European Union and/or for the clarification of provisions of this Law;

(lg) acts as the competent authority for the management of large-scale incidents and crises in the field of cybersecurity as the cyber crisis management authority;

(ii) receives notifications of serious incidents under the provisions of article 35B as well as cyber threat incidents and near misses under the provisions of article 42;

(lÿ) participates in peer reviews pursuant to the provisions of article 34A;

(m) uses the necessary means to exercise effective supervision of the entities falling within the scope of this Law and takes the necessary measures to ensure their compliance under the provisions of this Law; and

(ma) creates and maintains a register with DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content distribution network providers, managed service providers, managed security service providers as well as online marketplace providers, online search engine providers or social networking service platform providers, subject to the provisions of article 37A.";

Amendment of article 19 the basic law.

13. Article 19 of the basic law is amended as follows:

(a) By deleting paragraph (a) of subsection (1) and adding, immediately thereafter, the following new paragraph:

"(a1) the key and/or important entities and/or fixed and mobile communications providers, such as, subject to the provisions of subsections (2) and (3) of article 2 and if the Authority deems it appropriate upon request of the Police and/or the Cyprus Intelligence Service, provide the Authority and/or the Police and/or the Cyprus Intelligence Service with the necessary information for the purposes of public order and national security,";

(b) by amending paragraph (b) of subsection (1) as follows:

(i) by replacing the phrase "operators of essential services and/or critical information infrastructure operators" (first and second lines) with the phrase "key and/or important entities";

(ii) by adding immediately after the phrase "including, among other things, documented security policies" (fourth line), the phrase "to remedy any failure to comply and/or provide evidence";

(iii) by deleting the phrase "and/or elements" (fourth line);

Machine Translated by Google

(iv) by replacing the phrase “operators of essential services and/or critical information infrastructure operators” (tenth and eleventh lines) with the phrase “key and/or important entities”; and

(v) by replacing, immediately after the phrase "issued for the implementation of the provisions of this Law" (fourteenth line), the comma with a colon and adding, immediately after, the following proviso:

"It is understood that information obtained by the Authority, in accordance with the provisions of this subsection, concerns the promotion of the purposes referred to in the provisions of articles 15 and 16 and the execution of the responsibilities, powers and duties of the Authority referred to in the provisions of article 17 and may not be used for any purpose other than that for which it was requested.";

(c) by deleting paragraph (c) of subsection (1);

(d) by deleting the proviso to subsection (1);

(e) by amending paragraph (a) of subsection (2) as follows:

(i) by replacing the words “subsection (1)” (second line), with the words “this article”; and

(ii) by replacing the word “timely” (second line), with the phrase “within a specified period, subject to the provisions of article 18 and subsection (1) of article 19,”;

(f) by replacing in paragraph (b) of subsection (2) the phrase “operator of essential services and/or operator of critical information infrastructure, any provider of electronic communications networks and/or services and any digital service provider” (first to third lines), with the phrase “essential and/or significant entity”;

(g) by replacing paragraph (e) of subsection (2) with the following: paragraph:

“(e) Without prejudice to Article 346 of the Treaty on the Functioning of the European Union, information which is confidential, in accordance with Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other competent authorities in accordance with this Law only to the extent that such exchange is necessary for the application of this Law and the information exchanged shall be limited to what is relevant and proportionate to the purpose of such exchange, in order to:
preserves the confidentiality of such information and protects the security interests and commercial interests of the entities concerned.

(h) by replacing in paragraph (a) of subsection (3), the phrase “has valid reasons to judge differently” (third line), with the phrase “for the purposes of exercising its powers, decides differently and must document its Decision to disclose the information”; and

(i) by replacing in paragraph (b) of subsection (3) the phrase "critical information infrastructure operators, operators of essential services and digital service providers and/or providers of electronic communications networks and services" (second to fourth lines), with the phrase "key and/or important entities".

Amendment of article 20 the basic law.

14. Article 20 of the basic law is amended as follows:

(a) By amending subsection (1) as follows:

(i) by replacing in paragraph (a) the phrase "to operators of essential services, critical information infrastructure operators, digital service providers and network and/or service providers"

Machine Translated by Google

electronic communications" (third to fifth lines), with the phrase "in the main and/or important entities";

(ii) by amending paragraph (b) as follows:

(aa) by replacing the phrase “any operator of essential services, critical information infrastructure operator, digital service operator or provider of electronic communications networks and/or services” (first to third lines), with the phrase “any essential and/or significant entity”; and

(BB) by adding immediately after the phrase "and/or in external networks" (seventh line), the phrase ", without prejudice to the provisions of subsections (4) and (5) of article 31A";

(iii) by replacing in the proviso to paragraph (b) the phrase “only upon request and/or consent of the body or provider” (ninth line), with the phrase “only upon request of the basic and/or significant entity or its consent and/or for reasons of national security, subject to the provisions of subsection (3) of article 15”;

(iv) by replacing in paragraph (c) the phrase “digital security measures and procedures for notifying digital security breaches” (first and second lines), with the phrase “cybersecurity risk management measures and procedures for notifying digital security incidents”; and

(v) by replacing in paragraph (e) the phrase “to operators of essential services or critical information infrastructures or to digital service providers or to providers of electronic communications networks and/or services” (first to third lines), with the phrase “to essential and/or important entities”; and

(b) by replacing in subsection (2) thereof the phrase “electronic communications networks and systems, the provision/management of critical information infrastructures/basic information services or digital services,” (fourth to sixth lines), with the phrase “services from basic and important entities,”.

Amendment of article 23 the basic law.

15. Article 23 of the basic law is amended by replacing in subsection (1) the phrase “any operator of essential services/critical information infrastructure, digital service provider and provider of electronic communications networks and/or services” (second to fourth lines), with the phrase “any essential and/or significant entity”.

Amendment of article 24 the basic law.

16. Article 24 of the basic law is amended by replacing in paragraph (a) the phrase "operators of essential services, with digital service providers, with critical infrastructure operators or providers of electronic communications networks and/or services" (first to third lines) with the phrase "essential and/or important entities".

Amendment of article 26 the basic law.

17. Article 26 of the basic law is amended by replacing in paragraph (a) the phrase "interested body/provider" (second line) with the phrase "interested basic and/or significant entity".

Amendment the basic law with the replacement of the title of Part Seventh.

18. The principal law is amended by replacing the title of Part Seven with the following new title:

"KEY AND IMPORTANT ENTITIES"

Amendment the basic law with the replacement of article 27.

19. Article 27 of the basic law is replaced by the following article:

Machine Translated by Google

"Basic and Important Entities.

(1) (a) For the purposes of this Law, key entities the following entities are considered:

Annex I.

(i) entities of the types listed in Annex I, which exceed the thresholds for medium-sized enterprises set out in Article 2(1) of the Annex to Recommendation 2003/361/EC;

(ii) approved trust service providers and top-level domain name registries as well as service providers DNS, regardless of their size;

(iii) providers of public electronic communications networks or publicly available electronic communications services that qualify as medium-sized enterprises, pursuant to the provisions of Article 2 of the Annex to Recommendation 2003/361/EC;

(iv) public administration entities referred to in point (i) of paragraph (f) of subsection (2) of article 2A;

Annex I. Annex II.

(v) any other entities of the types referred to in Annex I or II, which are identified by the Authority as key entities pursuant to the provisions of paragraphs (b) to (e) of subsection (2) of section 2A;

(vi) entities that are identified as critical entities by the competent authority for the resilience of critical entities, referred to in the provisions of subsection (3) of article 2A; and

(vii) entities which the Authority designated, before 16 January 2023, as operators of essential services or as operators of critical information infrastructure, in accordance with the Commissioner's Decisions dated 17/08/2020 and 08/11/2021 issued or replaced pursuant to the provisions of the Network and Information Systems Security Law of 2020:

It is understood that the Commissioner's Decisions dated 17/8/2020 and 8/11/2021 continue to be in force until they are replaced, following a criticality assessment project, as provided for in paragraph (b) of subsection (1) of article 27; and

(b) For the purposes of implementing the provisions of paragraph (a) of subsection (1), and unless otherwise provided in this Law, the Authority may identify entities as key entities following a criticality assessment project, based on criteria determined by the Authority after consultation with the Deputy Minister, subject to the provisions of subsection (7) of this article:

It is understood that the criteria for the criticality assessment project are determined by the Authority and approved by a Decision of the Council of Ministers prior to their implementation and are valid until amended by a new Decision of the Council of Ministers.

Annex I. Annex II.

(2) For the purposes of this Law, entities of the types referred to in Annex I or II, which are not considered key entities in accordance with subsection (1), are considered significant entities and these include entities identified by the Authority as significant entities under paragraphs (b) to (e) of subsection (2) of section 2A.

(3) The Authority shall establish a list of key and significant entities as well as entities providing domain name registration services, which it shall review and, where appropriate, update on a regular basis and at least every two years.

(4) For the purposes of compiling the list referred to in subsection (3), the Authority shall require the entities referred to in that subsection to submit at least the following information to it:

Machine Translated by Google

(a) The name of the entity;

(b) address and up-to-date contact information, including email addresses, IP ranges and telephone numbers;

(c) where applicable, the relevant sector and sub-sector that referred to in Annex I or II; and

Annex I.
Annex II.

(d) where applicable, a list of the Member States in which they provide services falling within the scope of this Law:

It is understood that entities referred to in subsection (3) shall notify any changes to the information submitted in accordance with this subsection, without delay and, in any case, within two (2) weeks from the date of the change:

It is further understood that the Authority may establish national mechanisms for the entities themselves to register:

It is further understood that the Authority shall take into account guidelines and templates, which are established by the Commission, regarding the obligations set out in subsection (3).

(5) The Authority, every two years, shall notify:

(a) to the Commission and the Cooperation Group the number of key and significant entities listed in accordance with subsection (3) for each sector and subsector referred to in Annex I or II; and

Annex I.
Annex II.

(b) to the Commission relevant information on the number of key and significant entities identified under paragraphs (b) to (e) of subsection (2) of Article 2A, the sector and subsector referred to in Annex I or II to which they belong, the type of service they provide and the provision under which they were identified, among those specified in paragraphs (b) to (e) of subsection (2) of Article 2A.

Annex I.
Annex II.

(6) The Authority may, upon request of the Commission, communicate to the Commission the names of the key and significant entities referred to in paragraph (b) of subsection (5).

(7) The results of the assessment work carried out by the Authority as well as the list of key and significant entities, entities providing domain name registration services and entities exempted under subsection (4) of article 2 of this Law, which is prepared by the Authority under the provisions of this article, are approved by a Decision of the Council of Ministers, which is classified as confidential and is not published in the Official Gazette of the Republic:

It is understood that the results of the evaluation project and the list of key and significant entities as well as entities providing domain name registration services approved by the Decision of the Council of Ministers are confidential and are not published in the Official Gazette of the Republic.

(8) The key and significant entities approved by a Decision of the Council of Ministers pursuant to the provisions of subsection (7) are defined by a Decision issued by the Authority and served on the said key or significant entity.".

Machine Translated by Google

Amendment the basic law with the addition of the young articles 27A and 27B.

20. The basic law is amended by adding, immediately after article 27, the following new articles:

"Safety from the design (security by design).

27A. Newly established entities in the Republic, which fall within the scope of this Law and may be identified as key or significant entities, pursuant to the provisions of article 27, shall inform and seek the opinion and/or guidance of the Authority on the security measures they must take from the design/creation (security by design) of their IT infrastructures as well as the obligations to which they are subject from the day of commencement of the provision of their services, in compliance with the provisions of article 39.

Obligation information of the Authority.

27B. Without prejudice to the provisions of article 27, newly established entities and/or entities that fall within the scope of article 2A of this Law and were not included in the list of key and significant entities drawn up by the Authority in accordance with subsection (3) of article 27, must inform the Authority for the purposes of their assessment.".

Amendment the basic law with the deletion of article 28.

21. The basic law is amended by deleting article 28.

Amendment the basic law with the replacement of article 29.

22. Article 29 of the basic law is replaced by the following article:

"National strategy cybersecurity.

"(1)(a) The Deputy Minister shall determine the general policy framework in relation to digital security pursuant to the provisions of article 16 and shall forward to the Council of Ministers for approval the cybersecurity strategy, for the preparation of which he shall take seriously into account relevant recommendations and/or guidelines of the Authority.

(b) The cybersecurity strategic plan shall provide for the strategic objectives, the resources required to achieve those objectives, appropriate policy measures and regulatory measures with a view to achieving and maintaining a high level of cybersecurity and shall include at least the following:

Annex I. Annex II.

(i) Objectives and priorities covering in particular the areas referred to in Annexes I and II;

(ii) a governance framework for achieving the objectives and priorities referred to in paragraph (a) of this subsection, including the policies referred to in subsection (2);

(iii) a governance framework that clarifies the roles and responsibilities of relevant stakeholders at national level, which supports cooperation and coordination at national level with the Authority and the CSIRTs in the Republic as well as coordination and cooperation between these bodies and the competent authorities based on sectoral legal acts of the Union;

(iv) a mechanism for identifying relevant assets and assessing risks at national level;

Machine Translated by Google

(v) identifying measures to ensure preparedness, response and recovery from incidents, including cooperation between the public and private sectors;

(vi) a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;

(vii) a policy framework for enhanced coordination between the Authority and the competent authority in the Republic for the resilience of critical entities, for the purpose of exchanging information on risks, cyber threats and incidents as well as on risks, threats and incidents outside cyberspace and exercising supervisory duties, as appropriate; and

(viii) a plan, including the necessary measures, to enhance the general level of awareness and information of citizens in the field of cybersecurity.

(2) Within the framework of the national cybersecurity strategy and taking into account the provisions of article 16, the national strategy shall include at least the following policies-

(a) addressing cybersecurity in the supply chain of ICT products and ICT services used by entities to provide their services;

(b) including and specifying cybersecurity-related requirements for ICT products and ICT services in public procurement, including those related to cybersecurity certification, encryption and the use of open source cybersecurity products;

(c) vulnerability management, including the promotion and facilitation of coordinated vulnerability disclosure pursuant to the provisions of subsection (1) of section 31B;

(d) maintaining the general availability, integrity and confidentiality of the public core of the open internet, including, where appropriate, the cybersecurity of undersea communications cables;

(e) promoting the development and integration of relevant advanced technologies with a view to implementing advanced risk management measures in the field of cybersecurity;

(f) promoting and developing cybersecurity education and training, cybersecurity skills, awareness-raising and research and development initiatives as well as guidance on good cyber hygiene practices and controls, targeting citizens, stakeholders and entities;

(g) supporting academic and research institutions to develop, strengthen and promote the deployment of cybersecurity tools and secure network infrastructures;

(or) including relevant procedures and appropriate information exchange tools to support the voluntary exchange of cybersecurity information between entities in accordance with Union law;

(i) strengthening the cyber resilience and cyber hygiene baseline of small and medium-sized enterprises, especially those excluded from the scope of this Law by providing easy

Machine Translated by Google

accessible guidance and assistance for their special needs; and

(j) promoting active cyber protection (active cyber protection):

It is understood that active cyber protection, without limitation, consists of preventing, detecting, monitoring, analyzing and mitigating network security breaches in an active manner, in combination with the use of capabilities developed within and outside the entities' network:

It is further understood that the services of the Authority, taking into account, among others, the availability of the Authority's resources and/or the criticality, may include, at its discretion, the provision of free services or tools to certain entities and for a specific period of time, including self-service checks, detection tools, takedown services and sensor installation pursuant to the provisions of paragraph (b) of subsection (1) of article 20.

(3)(a) The Authority shall evaluate the national cybersecurity strategy on a regular basis and at least every four (4) years based on key performance indicators and shall recommend its updating.

(b) ENISA shall assist the Authority, upon its request, in the development or updating of the national cybersecurity strategy and the key performance indicators for the evaluation of said strategy, with a view to aligning it with the requirements and obligations set out in this Law.

(4)(a) The Authority shall notify the national cybersecurity strategy to the Commission within three (3) months of its approval.

(b) The Authority may exclude from such notification information relating to national security.”.

Amendment of article 30 the basic law.

23. Article 30 of the basic law is amended as follows:

(a) By replacing the side title with the following new side title:

"Competent national authority and single point of contact."

(b) by replacing in subsection (1) the phrase “for the security of networks and information systems and as a competent authority, it covers at least the sectors referred to in a Decision and the types of digital services referred to in a Decision issued by the Authority.” (third to fifth lines), with the phrase “for cybersecurity, it has the duties of supervision and enforcement as provided for in the provisions of this Law and has the duties of the cyber crisis management authority pursuant to the provisions of article 32A.”;

(c) by amending subsection (2) as follows:

(i) By adding, immediately after the phrase “continues to be” (fourth line), the word “competent”;

(ii) by adding, immediately after the phrase “for the coordination of the implementation of” (fourth and fifth lines), the word “national”; and

(iii) by deleting the phrase “and the competent authority for coordinating the implementation of the cybersecurity strategy” (fifth and sixth lines);

Machine Translated by Google

(d) by replacing subsection (4) with the following subsection:

"(4) The Authority is designated as the national single point of contact for cybersecurity ('single point of contact').";

(e) by amending subsection (5) as follows:

(i) by replacing the phrase "contact centre" (first line) with the phrase "contact point"; and

(ii) by replacing the phrase "the cooperation group and the CSIRT network, provided for in the provisions of Article 33." (second and third lines), with the phrase "and, where appropriate, with the Commission and the ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within the Republic.";

(f) by replacing in subsection (6) the phrase "The Commissioner and the Authority shall ensure that the Authority, as the competent authority and single point of contact, has adequate resources," (first and second lines), with the phrase "The Authority shall ensure that it has the necessary powers and adequate resources"; and

(g) by replacing subsection (7) with the following subsection:

"(7) In order to ensure the effective performance of the tasks and obligations of the Authority, as a competent authority and as a single point of contact, the Authority shall ensure, to the extent possible, appropriate cooperation between the competent national law enforcement authorities, the Cyprus Intelligence Service, the Commissioner for Personal Data Protection, the Department of Civil Aviation, the competent authorities under "Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No. 2111/2005, (EC) No. 1008/2008, (EU) No. 996/2010, (EU) No. 376/2014 and Directives 2014/30/EU and 2014/53/66 of the European Parliament and of the Council, and repealing Regulations (EC) No. 552/2004 and (EC) No. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No. 3922/91", the Department of Electronic Communications, the competent authorities of the Republic under Regulation (EU) 2022/2554, OCECPR, the Central Bank of Cyprus as the national macroprudential authority and the competent authority of the Republic for the resilience of critical entities, as well as the competent authorities under other sectoral legal acts of the Union, within the Republic.".

Official Newspaper of the EU: L212, 22.8.2018, p. 1.

Amendment the basic law with the replacement of article 31.

24. Article 31 of the basic law is replaced by the following article:

"Computer Security Incident Response Team" (national CSIRT).

31.-(1) The national CSIRT shall comply with the requirements set out in subsection (1) of section 31A, cover at least the sectors, sub-sectors and types of entities referred to in Annexes I and II and shall be responsible for handling incidents in accordance with a clearly defined procedure.

Annex I.
Annex II.

(2) The national CSIRT has an appropriate, secure and resilient communication and information infrastructure through which it exchanges

Machine Translated by Google

information with key and important entities and other relevant stakeholders and contributes to the development of secure information exchange and cybersecurity tools.

(3) The Authority shall ensure that the national CSIRT has sufficient resources for the effective performance of its tasks, pursuant to the provisions of subsection (4) of article 31A.

(4) The national CSIRT shall conclude memoranda of cooperation with relevant private sector stakeholders, with a view to achieving the objectives under the provisions of this Law.

(5) The national CSIRT shall cooperate and, where appropriate, exchange relevant information pursuant to the provisions of Article 34B with sectoral or cross-sectoral communities of key and important entities.

(6) The Authority shall ensure the effective, efficient and safe cooperation of the national CSIRT within the framework of the CSIRT Network.

(7) The national CSIRT shall participate in peer reviews pursuant to the provisions of Article 34A.

(8) The national CSIRT may cooperate with National Computer Security Incident Response Teams (CSIRTs) of a third country or with equivalent third country bodies, and where required through the Cyprus Intelligence Service, in particular with a view to providing assistance in the field of cybersecurity and/or implementing the provisions of paragraph (ld) of article 17:

It is understood that this cooperation as well as the exchange of relevant information with National Computer Security Incident Response Teams (CSIRTs) of a third country, including personal data, is carried out in accordance with the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Movement of Such Data Law and Regulation (EU) 2016/679.

(9) The Authority may request the assistance of ENISA for the development of the national and sectoral CSIRTs.

(10)(a) Regulation (EU) 2022/2554 is considered a sectoral legal act of the Union in relation to this Law as regards financial sector entities.

(b) Instead of the provisions established in this Law, the provisions of Regulation (EU) 2022/2554 on information and communication technology (ICT) risk management, ICT incident management and in particular the reporting of serious ICT incidents, as well as on digital operational resilience testing, information sharing arrangements and the risk of third-party ICT providers shall apply.

(c) The provisions of this Law regarding risk management obligations in the field of cybersecurity and incident reporting and supervision, as well as enforcement of the law, do not apply to financial entities covered by Regulation (EU) 2022/2554.

(11) The competent authorities of the Republic, pursuant to the provisions of Regulation (EU) 2022/2554, are expected to cooperate with the national CSIRT for large-scale incidents or cyber threats that have a significant impact with the aim of facilitating cross-sectoral learning and contributing to the prevention and management of cyberattacks.

(12) In order to maintain a close relationship and exchange of information with the financial sector, the European Supervisory Authorities

Machine Translated by Google

Authorities (ESAs) and the competent authorities under the provisions of Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group, exchange information and cooperate with the Authority.".

Amendment the basic law with the addition of new articles 31A and 31B.

25. The basic law is amended by adding, immediately after article 31, the following new articles:

"Requirements, techniques abilities and his duties national CSIRT.

31A.-(1) The national CSIRT shall comply with the following requirements:

(a) ensures a high level of availability of its communication channels, avoiding single points of failure and has various ways for incoming and outgoing communication with third parties at all times, clearly identifies the communication channels and communicates them to the entities supervised by the Authority and to cooperating partners;

(b) the national CSIRT's premises and supporting information systems are located in secure areas;

(c) is equipped with an appropriate request management and routing system, in particular to facilitate the effective and efficient delivery of tasks;

(d) ensures the confidentiality and reliability of its activities;

(e) is sufficiently staffed to ensure the availability of its services at all times and ensures that its personnel are appropriately trained;

(f) is equipped with redundant systems and a backup workspace to ensure the continuity of its services.

(2) The national CSIRT may participate in international cooperation networks.

(3)(a) The Authority shall ensure that the national CSIRT has the technical capabilities required to perform the tasks provided for in subsection (4).

(b) The Authority shall ensure that the national CSIRT has sufficient resources to ensure adequate staffing levels to be able to develop its technical capabilities.

(4) The national CSIRT is tasked with the following tasks:

(a) Monitoring and analysis of cyber threats, vulnerabilities and incidents at national level and, upon request and/or pursuant to the provisions of subsection (3) of article 15, providing assistance to affected key and important entities regarding the monitoring of their network and information systems in real time or near real time;

(b) providing timely warnings, notifications, announcements and dissemination of information to key and important entities involved, as well as to competent authorities, other relevant stakeholders and other interested parties at the discretion of the Authority,

Machine Translated by Google

about cyber threats, vulnerabilities and incidents, if possible, in near real time;

(c) incident response and assistance to affected key and significant entities, as appropriate;

(d) collection and analysis of forensic data and dynamic risk and incident analysis and situational awareness in cybersecurity matters;

(e) providing, upon request of a key or significant entity, proactive scanning and/or penetration testing of that entity's network and information systems to identify vulnerabilities with a potential significant impact;

(f) participating in the CSIRT Network and providing mutual assistance in accordance with its capabilities and responsibilities to other members of the CSIRT Network upon their request;

(g) assuming a coordinating role for the purposes of the coordinated vulnerability notification process pursuant to subsections (1) and (2) of article 31B;

(h) contributing to the development of secure information exchange and cybersecurity tools in accordance with subsection (2) of article 31:

It is understood that, when performing the tasks referred to in this paragraph, the national CSIRT may prioritize specific tasks within the framework of a risk-based approach.

(5)(a) The national CSIRT may conduct proactive non-intrusive scanning of publicly accessible network and information systems of key and important entities.

(b) Such scanning is carried out to identify vulnerable or insecurely configured network and information systems and to inform said entities.

(c) Such scanning has no negative consequences for the operation of the entities' services.

(6) In order to facilitate the cooperation referred to in paragraph (4) of Article 31, the national CSIRT shall promote the adoption and use of common or standardized practices, classification schemes and taxonomies in relation to-

(a) incident handling procedures;

(b) crisis management; and

(c) coordinated notification of vulnerabilities pursuant to the provisions of subsections (1) and (2) of article 31B.

Coordinated vulnerability disclosure and European vulnerability database.

31B.-(1) For the purposes of coordinated vulnerability reporting, the national CSIRT shall act as a coordinator, and, in application of its coordination tasks, shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting the vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon request of one of the parties.

Machine Translated by Google

(2) The tasks of the national CSIRT include:

(a) Identification of the entities involved and communication with them;

(b) the provision of assistance to natural or legal persons who report vulnerabilities; and

(c) negotiating disclosure schedules and managing vulnerabilities affecting multiple entities.

(3)(a) The Authority shall ensure that natural or legal persons may report vulnerabilities anonymously, upon request, to the national CSIRT.

(b) The national CSIRT ensures that diligent follow-up actions are carried out regarding the reported vulnerability and ensures the anonymity of the natural or legal person reporting the vulnerability.

(c) In cases where a reported vulnerability may have a significant impact on entities in more than one Member State, the national CSIRT shall cooperate, where appropriate, with other CSIRTs assigned a coordination role within the CSIRT network.

(4) The Authority may make publicly available and register on a voluntary basis in the European database developed and maintained by ENISA pursuant to the provisions of Article 12 of Directive (EU) 2022/2555, publicly known vulnerabilities in ICT products or ICT services.".

Amendment the basic law with the replacement of article 32.

26. Article 32 of the basic law is replaced by the following article:

"Cooperation in national level.

32.-(1) The Authority, as a competent authority and as a single point of contact and as the national CSIRT, cooperates with the sectoral CSIRTs and other competent authorities for the purposes of complying with the obligations provided for in the provisions of this Law.

(2) The Authority shall receive notifications of serious incidents pursuant to the provisions of article 35B as well as of cyber threat incidents and near misses pursuant to the provisions of article 42.

(3) The Authority, as a single point of contact, for the fulfillment of its duties, shall be kept informed of notifications of incidents, cyber threats and near-misses submitted under the provisions of this Law and subject to the provisions of subsection (l) of article 17, subsection (7) of article 30 and subsection (10) of article 31.

(4)(a) The Authority and the competent authority for the resilience of critical entities shall cooperate and exchange information on a regular basis regarding the identification of critical entities, risks, cyber threats and incidents, as well as risks, threats and incidents outside cyberspace, affecting key entities identified as critical entities by the competent authority for the resilience of critical entities and the measures taken to address such risks, threats and incidents.

(b) The competent authorities of the Republic under Regulation (EU) 2022/2554, OCECPR and the Department of Electronic Communications, the Central Bank of Cyprus as the national macroprudential authority and

Machine Translated by Google

other competent authorities, exchange relevant information with the Authority on a regular basis, including with regard to relevant incidents and cyber threats.

(5) The Authority shall simplify the submission of notifications by technical means. referred to in articles 35B and 42 of this Law.".

Amendment the basic law with the addition of article 32A.

27. The basic law is amended by adding, immediately after article 32, the following new article:

"National framework" management cyber crises.

32A.-(1) The Authority, as the competent authority for the management of large-scale incidents and crises in the field of cybersecurity (cyber crisis management authority), shall ensure that it has sufficient resources for the effective and efficient performance of its duties under this Law and that there is coherence with the existing frameworks for general national crisis management in the field of cybersecurity.

(2) The Authority acts as a coordinator in the management of large-scale incidents and crises in the field of cybersecurity, in cooperation with the competent authorities of the Republic under the respective laws of the Republic or sectoral legal acts of the Union:

It is understood that, in cases where the financial sector is involved, the Authority acts as a coordinator in cooperation with the Central Bank of Cyprus as the National Macroprudential Authority.

(3) The Authority shall determine the capabilities, assets and procedures that may be used in the event of a crisis for the purposes of this Law.

(4) The Authority shall establish a national plan for responding to large-scale incidents and crises in the field of cybersecurity, which shall set out the objectives and arrangements for the management of large-scale incidents and crises in the field of cybersecurity.

(5) The national plan for responding to large-scale incidents and crises in the field of cybersecurity is approved by a Decision of the Council of Ministers, which is classified as confidential and is not published in the Official Gazette of the Republic.

(6) The said plan shall specify in particular-

(a) the objectives of national preparedness measures and activities;

(b) the duties and responsibilities of the Authority, as a cyber crisis management authority;

(c) cyber crisis management procedures, including their integration into the overall national crisis management framework and information exchange channels;

(d) national preparedness measures, including exercises and training activities;

(e) relevant public and private sector stakeholders and relevant infrastructure; and

(f) the national procedures and arrangements between the competent national authorities and bodies to ensure the effective participation and provision of support by the Republic in the coordinated management of large-scale incidents and crises in the field of cybersecurity at Union level.

Machine Translated by Google

(7) The Authority shall submit to the Commission and the European Network of Cyber Crisis Liaison Organizations (EU-CyCLONe) relevant information on the provisions of subsection (4) of this article regarding the national plan for responding to large-scale incidents and crises in the field of cybersecurity, within three months of the approval of that plan.

(8) The Authority may, upon approval of the Council of Ministers, exempt specific information when and to the extent that such exemption is necessary for national security purposes.

(9) The Authority may request contribution to the national plan for responding to large-scale incidents and crises from the European Network of Cyber Crisis Liaison Organizations (EU-CyCLONe), in accordance with point (e) of paragraph (3) of Article 16 of Directive (EU) 2022/2555.".

Amendment the basic law with the replacement of the title of Part Ninth.

28. The basic law is amended by replacing the title of Part Nine as follows:

"COLLABORATION AND PEER REVIEWS".

Amendment of article 33 the basic law.

29. Article 33 of the basic law is amended as follows:

(a) By replacing the side title with the following new side title:

“Cooperation Group, CSIRT Network and European Network of Liaison Organizations for Cyber Crisis (EU-CyCLONe).”

(b) by replacing subsection (1) as follows:

"(1) Representatives of the Authority, and pursuant to paragraph (2) of Article 8 of Directive (EU) 2022/2555, shall participate in the Cooperation Group, which has been established and operates under the provisions of Article 14 of Directive (EU) 2022/2555 and shall contribute to the relevant work of the Cooperation Group, including, inter alia, Articles 14 and 22 of Directive (EU) 2022/2555.";

(c) by amending subsection (2) as follows:

(i) by replacing the phrase “national CSIRT network” (first line) with the phrase “CSIRT Network”; and

(ii) by replacing the phrase “Article 12 of Directive 2016/1148/EU” (second line) with the phrase “Article 15 of Directive (EU) 2022/2555”;

(d) by adding, immediately after subsection (3), the following new subsection:

"(4) Subject to the provisions of article 32A, representatives of the Authority shall participate in the EU-CyCLONe established under the provisions of article 16 of Directive (EU) 2022/2555 and shall actively contribute to its relevant work.".

Amendment of article 34 the basic law.

30. Article 34 of the basic law is amended by adding, immediately after paragraph (b), the following new paragraph:

"(c) to participate effectively in exchange programmes for officials from other Member States, within a specific framework and, where appropriate, taking the necessary measures."

Machine Translated by Google

security clearance of officers participating in these exchange programmes, with a view to improving cooperation and strengthening the trust of Member States.

Amendment the basic law with the addition of new articles 34A, 34B and 34C.

31. The basic law is amended by adding, immediately after article 34, the following new articles:

"Evaluations" from peers.

34A.-(1)(a) The Authority participates in peer reviews and its participation in them is voluntary.

(b) Peer reviews are carried out pursuant to the provisions of Article 19 of Directive (EU) 2022/2555, by experts in the field of cybersecurity.

(c) Experts in the field of cybersecurity shall be designated by at least two (2) Member States, other than the Member State under consideration.

(2) Peer reviews shall cover at least one of the following:

(a) the level of implementation of cybersecurity risk management measures and incident reporting obligations provided for in Articles 21 and 23 of Directive (EU) 2022/2555;

(b) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the performance of tasks by the competent authorities;

(c) the operational capabilities of CSIRTs;

(d) the level of implementation of mutual assistance provided for in Article 37 of Directive (EU) 2022/2555;

(e) the level of implementation of the information exchange arrangements in the field of cybersecurity provided for in Article 29 of Directive (EU) 2022/2555; and

(f) specific issues of a cross-border or cross-sectoral nature.

(3)(a) The Authority shall appoint experts in the field of cybersecurity to be selected to conduct peer reviews based on objective, impartial, fair and transparent criteria in accordance with the methodology developed by the Cooperation Group, as provided for in paragraph (1) of Article 19 of Directive (EU) 2022/2555.

(b) The Commission and ENISA shall participate as observers in the peer reviews.

(4) The Authority may specify specific issues as referred to in paragraph (f) of subsection (2) for the purposes of peer review.

(5) Before the start of the peer review, as provided for in the provisions of subsection (1), the Authority shall notify the participating Member States of the scope of the review, including the specific issues identified under subsection (4).

Machine Translated by Google

(6)(a) Before the start of the peer review, the Authority may conduct a self-assessment of the aspects being assessed and provide said self-assessment to the designated cybersecurity experts.

(b) The Authority shall apply the methodology for the self-assessment as determined by the Cooperation Group, with the assistance of the Commission and ENISA.

(7)(a) Peer reviews include physical or virtual on-site visits and off-site exchanges of information.

(b) In accordance with the principle of good cooperation, the Authority, when subject to peer review, shall provide the designated cybersecurity experts with the information necessary for the review, without prejudice to Union law or applicable legislation on the protection of confidential or classified information and the safeguarding of essential functions of the State, such as national security.

(c) Any information obtained through the assessment by peers is used exclusively for this purpose.

(d) Cybersecurity experts participating in the peer review shall not disclose to third parties any sensitive or confidential information obtained during such peer review:

It is understood that the experts in the field of cybersecurity appointed by the Authority shall take into account the codes of conduct issued by the Cooperation Group in cooperation with the Commission and ENISA.

(8) Peer-reviewed items shall not be subject to further peer review for a period of two (2) years after the completion of the review, unless otherwise decided by the reviewee or agreed upon by the Collaboration Group.

(9)(a) The Authority shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is disclosed to the other Member States, the Cooperation Group, the Commission and ENISA, before the start of the peer review.

(b) The Authority, when subject to peer review, may object to the designation of specific experts for duly justified reasons which it shall communicate to the Member State designating the expert.

(10)(a) Cybersecurity experts participating in peer reviews shall draw up reports with the findings and conclusions of the reviews, which shall include recommendations allowing for the improvement of the aspects covered by the peer review.

(b) The Authority may submit comments on the draft reports that concern it and these comments shall be attached to the reports.

(c) Reports are submitted to the Cooperation Group and the Network CSIRT, as appropriate.

(d) The Authority may make public the report concerning it or a redrafted version thereof.

Machine Translated by Google

Settings for the exchange information in the field of cybersecurity.

34B.-(1) The key and significant entities falling within the scope of this Law and, where applicable, other entities not falling within the scope of this Law may exchange with each other, on a voluntary basis, information relevant to cybersecurity, including information relating to cyber threats, near-misses, vulnerabilities, techniques and procedures, indicators of compromise, hostile tactics, threat actor specific information, cybersecurity warnings and recommendations on the configuration of cybersecurity tools for detecting cyber attacks, to the extent that such exchange of information-

(a) aims to prevent, detect, respond to or recover from incidents or mitigate their impact;

(b) enhances the level of cybersecurity, in particular through awareness-raising about cyber threats, limiting or hindering the ability of these threats to spread, supporting a range of defensive capabilities, remediation and vulnerability disclosure, threat detection, containment and prevention techniques, mitigation strategies or response and recovery phases, or promoting collaborative research on cyber threats between public and private actors.

(2)(a) The exchange of information shall take place within the framework of communities of key and significant entities and, where applicable, their suppliers or service providers.

(b) The exchange of information shall be carried out through arrangements for the exchange of information in the field of cybersecurity with regard to the potentially sensitive nature of the information exchanged.

(3)(a) The Authority shall establish arrangements for the exchange of information in the field of cybersecurity referred to in the provisions of subsection (2).

(b) Such arrangements may specify operational elements, including the use of specific ICT platforms and automation tools, the content and terms of information exchange arrangements.

(c) When determining the details of the participation of public authorities in such arrangements, the Authority may impose conditions regarding the information made available by it.

(d) The Authority shall provide assistance for the implementation of such arrangements in accordance with the policies referred to in paragraph (h) of subsection (2) of article 29.

(4) Key and significant entities shall notify the Authority of their participation in the information exchange arrangements in the field of cybersecurity referred to in subsection (2), immediately after the conclusion of such arrangements or, where applicable, of the withdrawal of their participation in such arrangements, as soon as it is concluded.

(5) The Authority shall take into account the best practices and guidance that ENISA may provide pursuant to the provisions of paragraph 5 of Article 29 of Directive (EU) 2022/2555.

Mutually subscription.

34C.-(1)(a) Where an entity provides services in more than one Member State or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the Authority shall cooperate with the competent authorities

Machine Translated by Google

of the Member States concerned and provide mutual assistance, as necessary.

(b) This cooperation implies, at least, that:

(i) In the event that the Authority applies supervisory or enforcement measures in the Republic, it shall inform and consult with the competent authorities of the other Member States concerned regarding the supervisory and enforcement measures it takes and vice versa;

(ii) the Authority may request another competent authority to take supervisory or enforcement measures and vice versa;

(iii) the Authority, upon receipt of a substantiated request from another competent authority, shall provide the other competent authority with mutual assistance commensurate with its own resources, so that supervisory or enforcement measures can be applied in an effective, efficient and consistent manner and vice versa:

It is understood that the mutual assistance referred to in subparagraph (iii) may cover requests for information and supervisory measures, including requests to conduct on-site inspections or off-site supervision or targeted safety checks:

It is further understood that, when the Authority receives a request for assistance, it shall not reject such request, unless it is established that it is not competent to provide the requested assistance, that the requested assistance is not proportionate to its supervisory duties or that the request concerns information or involves activities which, if communicated or executed, would be contrary to the essential interests of national security, public security or defence of the Republic:

It is further understood that, before rejecting such a request, the Authority shall consult the other relevant competent authorities, as well as, at the request of one of the Member States concerned, the Commission and ENISA.

(2) Where appropriate and by mutual agreement, the Authority may undertake joint supervisory actions with other competent authorities of different Member States.".

Amendment the basic law with the replacement of the title of Part Tenth.

32. The principal law is amended by replacing the title of Part Ten as follows:

"RISK MANAGEMENT MEASURES IN THE FIELD OF CYBERSECURITY, INCIDENT REPORTING OBLIGATIONS, SUPERVISION AND ENFORCEMENT"

Amendment the basic law with the replacement of article 35.

33. Article 35 of the basic law is replaced by the following article:

"Management measures" risks in the sector of cybersecurity.

35.-(1)(a) Key and significant entities shall take appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of network and information systems that they use for their activities or for the provision of their services and to prevent or minimise the impact of incidents on the recipients of their services or on other services.

Machine Translated by Google

(b) Taking into account the most recent technical capabilities (state-of-the-art) and, where applicable, the relevant European and international standards as well as the cost of implementation, the measures referred to in paragraph (a) of subsection (1), the key and significant entities shall ensure that the level of security of network and information systems is proportionate to the risk in question.

(c) When assessing the proportionality of such measures, due account shall be taken of the entity's degree of exposure to risks, the size of the entity and the likelihood of incidents occurring and their severity, including their social and economic impact.

(2) The measures referred to in paragraph (a) of subsection (1), which may be determined in a Decision issued by the Authority, shall be based on a holistic risk approach aimed at protecting network and information systems and the physical environment of such systems from incidents and shall include at least the following:

(a) Policies for risk analysis and information systems security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) acquiring, developing and maintaining network and information systems, in secure ways and means, including handling and disclosing vulnerabilities;

(f) policies and procedures for assessing the effectiveness of cybersecurity risk management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(or) policies and procedures regarding the use of cryptography and, where applicable, encryption;

(i) human resource security, access control policies and asset management; and

(j) use of multi-factor authentication or continuous authentication solutions, secure voice communications, video and text communications, and secure emergency communications systems within the entity, as appropriate.

(3) With regard to the measures referred to in paragraph (d) of subsection (2), entities shall take into account-

(a) the vulnerabilities that characterize each direct supplier and service provider and the overall

Machine Translated by Google

quality of the products and cybersecurity practices of their suppliers and service providers, including their secure development processes; and

(b) the results of the coordinated risk assessments of critical supply chains carried out in accordance with paragraph 1 of Article 22 of Directive (EU) 2022/2555.

(4) An entity which finds that it does not comply with the measures provided for under the provisions of subsection (2) shall be obliged to take all necessary, appropriate and proportionate corrective measures without delay.

(5) The Authority shall implement any implementing acts of the Commission to determine the technical and methodological requirements of the risk management measures referred to in subsection (2), in accordance with the provisions of paragraph 5 of Article 21 of Directive (EU) 2022/2555.".

Amendment the basic law with the addition of the young articles 35A and 35B.

34. The basic law is amended by adding, immediately after article 35, the following new articles:

"Governance" (Governance).

35A.-(1) The senior management of key and significant entities is required to approve the cybersecurity risk management measures taken by such entities in order to comply with the provisions of article 35, to oversee their implementation and may be held accountable for the entities' breach of the obligations under that article.

(2) The application of the provisions of subsection (1) does not affect the relevant legislation regarding the rules on liability applicable to public organizations, as well as the liability of public servants and elected or appointed officials.

(3) The members of the senior management of key and significant entities are required to attend training and offer similar training to their employees on a regular basis, in order to acquire sufficient knowledge and skills that allow them to identify risks and evaluate risk management practices in the field of cybersecurity and their impact on the services provided by the entity.

Liabilities notification incidents.

35B.-(1)(a) Key and significant entities shall notify the Authority without delay, subject to the provisions of subsection (4), of any incident that has a significant impact on the provision of their services, as referred to in subsection (3) (significant incident).

(b) Where appropriate, such entities shall notify, without undue delay, the recipients of their services of significant incidents that may adversely affect the provision of their services.

(c) Such entities shall report, inter alia, any information that allows the Authority to determine any cross-border implications of the incident.

(d) The act of notification does not entail increased liability on the part of the notifying entity.

(e) In the event that the said entities notify the Authority of a significant incident in accordance with paragraphs (a) to

Machine Translated by Google

(d) of subsection (1), the Authority shall forward the notification to the national CSIRT upon receipt.

(f) The Authority, as a single point of contact, in the event of a cross-border or cross-sectoral significant incident, shall ensure that it receives the relevant information communicated in accordance with subsection (4) in a timely manner and, whenever the Authority deems it necessary, in consultation with other competent authorities.

(g) The procedures and content of the incident notification, as well as any relevant information, are regulated by a Decision issued by the Authority, pursuant to the provisions of this Law.

(2) Where applicable, key and significant entities shall promptly notify recipients of their services who may be affected by a significant cyber threat of any measures or remedial actions they may take to address the specific threat and, where applicable, those entities shall inform recipients of their services of the significant cyber threat:

It is understood that, without prejudice to subsection (7), in the event that there is a serious reason for not informing the recipients, the entity must inform, consult and obtain approval from the Authority.

(3) An incident is considered significant if-

(a) has caused or may cause serious operational disruption of services or financial loss to that entity; and/or

(b) has affected or may affect other natural or legal persons, causing significant material or non-material damage.

(4) For the purposes of notification under subsection (1), the key and important entities submit to the Authority-

(a) without undue delay and in any event within six (6) hours of becoming aware of the significant incident, information, which, where appropriate, states whether there is a suspicion that the significant incident was caused by illegal or malicious actions or may have a cross-border impact;

(b) without undue delay and in any event within seventy-two (72) hours of the significant incident becoming aware of it, an incident notification, which, where applicable, updates the information referred to in paragraph (a) and states an initial assessment of the significant incident, including its severity and impact and, where applicable, the indications of the breach;

(c) at the request of the Authority, an interim report on relevant updates to the situation;

(d) a final report no later than one month after the submission of the incident notification in accordance with paragraph (b) or (f), which includes the following:

(i) Detailed description of the incident, including its severity and impact
ofÿ

(ii) the type of threat or root cause that may have caused the incident;

Machine Translated by Google

(iii) implemented and ongoing mitigation measures; and

(iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of submission of the final report referred to in paragraph (d), the key and significant entities shall submit a progress report every fifteen (15) days, after the submission of the incident notification in accordance with paragraph (b) or (f), until the submission of the final report which shall be submitted within fifteen (15) days of the restoration of the operation of the affected network or information system; and

(f) By way of derogation from paragraph (b), the trust service provider shall notify the Authority, regarding significant incidents affecting the provision of its trust services, without undue delay and in any case within twenty-four (24) hours from the moment it became aware of the significant incident.

(5)(a) The Authority shall provide the notifying entity, without delay and if possible within twenty-four (24) hours of receipt of the early warning referred to in paragraph (a) of subsection (4), with a response including initial feedback on the significant incident and, upon request by the entity, guidance or operational advice on the implementation of possible mitigation measures.

(b) The national CSIRT shall provide additional technical support if requested by the notifying entity or if deemed necessary by the Authority.

(c) In the event that there are suspicions that the significant incident concerns the commission of a criminal offence, the Authority also provides guidance on the notification of the significant incident to the Police.

(6)(a) Where appropriate, and in particular where the significant incident concerns two or more Member States, the Authority shall without delay inform the other affected Member States and ENISA of the significant incident.

(b) Such information includes the type of information received pursuant to subsection (4).

(c) In the above context, the Authority safeguards, in accordance with Union law or applicable legislation, the security and commercial interests of the entity as well as the confidentiality of the information provided.

(7) Where public awareness is necessary to prevent a major incident or to address an ongoing major incident, or where disclosure of the major incident is in the public interest, the Authority and, where appropriate, the competent authorities or CSIRTs of other Member States concerned, may, after consultation with the affected entity, inform the public about the major incident or require that entity to do so.

(8) The Authority, as a single point of contact, shall forward, where appropriate, the notifications received in accordance with subsection (1) to the single points of contact of other affected Member States.

Machine Translated by Google

(9)(a) The Authority shall submit to ENISA every three (3) months a summary report, which shall include anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified pursuant to the provisions of subsection (1) and the provisions of article 42 of this Law.

(b) The Authority shall take into account any technical guidance issued by ENISA on the parameters of the information to be included in the summary report.

(10) The Authority shall provide the competent authority for the resilience of critical entities with information on significant incidents, incidents, cyber threats and near-misses notified pursuant to the provisions of subsection (1) and the provisions of article 42 by entities identified as critical entities by the competent authority for the resilience of critical entities.

(11) The Authority shall implement the implementing acts adopted by the Commission in accordance with the provisions of paragraph (11) of Article 23 of Directive (EU) 2022/2555.

(12)(a) Where the provisions of a sectoral Union legal act require key or significant entities to comply with notification obligations which are at least equivalent in effect to the notification obligations set out in this Law, the consistency and effectiveness of the handling of incident notifications shall be ensured.

(b) To this end, the provisions of the sectoral Union legal act on the notification of occurrences should provide the Authority with direct access to the notifications of occurrences submitted in accordance with the sectoral Union legal act and, in particular, such direct access can be ensured if the notifications of occurrences are transmitted to the Authority without delay.

(c) Where appropriate, the Authority must establish an automatic and direct reporting mechanism that ensures the systematic and direct exchange of information regarding the handling of such incident notifications.

(d) For the purposes of simplifying notification and implementing the automatic and direct reporting mechanism, the Authority may, in accordance with the sectoral Union legal act, use a single entry point.

Amendment of article 36 the basic law.

35. Article 36 of the basic law is amended as follows:

(a) By replacing the side title with the following new side title:

"Supervision and enforcement.";

(b) by replacing subsections (1), (2) and (3) with the following subsections:

“(1) The Authority shall use the necessary means to exercise effective supervision of the entities falling within the scope of this Law and shall take the necessary measures to ensure their compliance with this Law.

(2) The Authority may issue a Decision on the manner of assessing the compliance of key and significant entities which fall within the scope of this Law with their obligations.

(3)(a) The Authority may prioritize the supervisory tasks and this prioritization is based on a risk-based approach.

Machine Translated by Google

(b) For this purpose, in the exercise of its supervisory duties, as provided for in articles 36A and 36B, the Authority may establish by its Decision, supervisory methodologies that allow for the prioritization of such duties with a risk-based approach.";

(c) By deleting subsections (4), (5) and (6);

(d) By replacing subsection (7) with the following subsection:

(7) When dealing with incidents leading to personal data breaches, the Authority shall cooperate closely with the Commissioner for Personal Data Protection, without prejudice to the resulting competence and duties under Regulation (EU) 2016/679."

(e) By adding, immediately after subsection (7), the following new subsection:

"(8)(a) Without prejudice to the legislative and institutional framework of the Republic, the Authority, in the exercise of its responsibilities and in particular in the supervision of the compliance of public administration entities and the provision and implementation of enforcement measures for violations of this Law, is functionally independent and exercises its powers and duties with functional independence vis-à-vis the supervised public administration entities.

(b) The Authority may decide to impose appropriate, proportionate and effective supervisory and enforcement measures in relation to such entities in accordance with the national legislative and institutional framework.".

Amendment the basic law with the addition of new articles 36A and 36B.

36. The basic law is amended by adding, immediately after article 36, the following new articles:

"Supervision measures" and enforcement basic entities.

36A.-(1) Supervisory or enforcement measures imposed on key entities, in relation to the obligations set out in this Law for key entities, shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

(2) The Authority, in exercising its supervisory functions in relation to key entities, has the power to subject such entities to at least-

(a) on-site inspections and off-site supervision, including random checks, carried out by qualified professionals;

(b) regular and targeted security audits carried out by the Authority or by a specialized independent body authorized by the Authority:

It is understood that the targeted security audits and their frequency referred to in this paragraph are based on risk assessments carried out by the Authority or the audited entity or on other risk-related information available:

It is further understood that the results of each targeted security audit shall be made available to the Authority and the cost of such targeted security audit, which shall be carried out by an independent body, shall be covered by the audited entity, except in duly justified cases for which the Authority decides otherwise;

Machine Translated by Google

(c) extraordinary special inspections, including when justified due to a significant incident or violation
the provisions of this Law by the main entity;

(d) security scans based on objective, impartial, fair and transparent risk assessment criteria, where required with the cooperation of the key entity;

(e) requests for information necessary to assess the cybersecurity risk management measures taken by that entity, including documented cybersecurity policies as well as compliance with the obligation to transmit information to competent authorities under the provisions of Article 37A;

(f) requests for access to data, documents and information necessary to carry out their supervisory tasks;

(g) requests for evidence relating to the implementation of cybersecurity policies, such as the results of security audits carried out by an authorized auditor as such authorization may be determined in a Decision of the Authority and/or an independent auditor, and the corresponding underlying evidence.

(3) The Authority, when exercising its powers as provided for in paragraphs (e), (f) or (g) of subsection (2), shall state the purpose of the request and specify the information requested.

(4) The Authority, in exercising its supervisory duties in relation to the basic entities, has the power at least to-

(a) issues warnings regarding violations of the provisions of this Law by key entities;

(b) issues binding instructions, including regarding the measures necessary to prevent or remedy an incident, as well as deadlines for the implementation of such measures and for the submission of reports on their implementation, or a Decision requesting the entities in question to remedy the deficiencies identified or the violations of the provisions of this Law;

(c) requires such entities to cease conduct that violates the provisions of this Law and to refrain from repeating such conduct;

(d) requires those entities to ensure that their cybersecurity risk management measures comply with Article 35 or to fulfil the reporting obligations provided for under the provisions of Article 35B, in a specified manner and within a specified period of time;

(e) requires such entities to inform natural or legal persons in relation to whom they provide services or carry out activities that may be affected by a significant cyber threat about the nature of the threat, as well as about any protective or remedial measures that they can take.

Machine Translated by Google

those natural or legal persons to address that threat;

(f) requires those entities to implement the recommendations made as a result of a security audit within a reasonable period of time;

(g) appoint a monitoring officer with clearly defined tasks for a specified period of time to oversee the compliance of those entities under the provisions of Articles 35 and 35B;

(or) requires such entities to disclose aspects of violations of the provisions of this Law in a specified manner; and

(i) imposes an administrative fine pursuant to the provisions of article 43A in addition to any of the measures referred to in paragraphs (a) to (h) of this subsection.

(5) In a case where the enforcement measures adopted in accordance with paragraphs (a) to (d) and (f) of subsection (4) are ineffective, the Authority has the power to set a deadline within which the principal entity is required to take the necessary measures to remedy the deficiencies or to comply with the Authority's requirements and if the requested measures are not taken within the specified deadline, the Authority has the power to-

(a) temporarily suspend or request from a certification or authorization body or a court, in accordance with applicable law, the temporary suspension of certification or authorization concerning part or all of the relevant services provided or activities performed by the main entity; and

(b) requests the competent authorities, in accordance with applicable law, to temporarily prohibit any natural person responsible for exercising management functions at the level of managing director or legal representative in the main entity from exercising management functions in that entity:

It is understood that temporary suspensions or prohibitions imposed pursuant to this subsection shall apply only until the entity in question takes the necessary measures to correct the deficiencies or comply with the requirements of the Authority for which such enforcement measures were applied:

It is further understood that the imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural guarantees in accordance with the general principles of Union law and the Charter of Fundamental Rights of the EU where it applies, including the right to effective judicial protection and fair trial, the presumption of innocence and the rights of the defence:

It is further understood that the enforcement measures provided for in this subsection do not apply to public administration bodies subject to this Law.

(6) Any natural person who is responsible for or acts as a legal representative of a key entity by virtue of the power to represent it, the authority to take decisions on its behalf or to exercise control over it, has the power to ensure its compliance with the provisions of this Law and the said

Machine Translated by Google

A natural person may be held liable for a breach of his obligations to ensure compliance with this Law:

It is understood that the application of this subsection does not affect the existing legislation regarding the rules on liability applicable to public organizations as well as the liability of public servants and elected or appointed officials.

(7) In a case where the Authority takes any of the enforcement measures referred to in subsections (4) or (5), it shall respect the rights of the defence and take into account the circumstances of each individual case and, at least, shall take due account of-

(a) the seriousness of the violation and the importance of the provisions violated, while in any case the following, among others, are considered serious violations:

(i) The existence of repeated violations;

(ii) failure to report or remedy significant incidents;

(iii) failure to remedy deficiencies in accordance with binding instructions from the Authority;

(iv) obstructing inspections or monitoring activities ordered by the Authority after an infringement has been detected; and

(v) providing false or grossly inaccurate information in relation to the risk management measures or the notification obligations set out in the provisions of Articles 35 and 35B;

(b) the duration of the infringement;

(c) any relevant previous violations by that entity;

(d) any material or non-material damage caused, including financial or economic damage, the impact on other services and the number of users affected;

(e) any intent or negligence on the part of the perpetrator of the infringement;

(f) any measures taken by the entity to prevent or mitigate material or non-material damage;

(g) any adherence to approved codes of conduct or approved certification mechanisms; and

(or) the degree of cooperation of the responsible natural or legal persons with the Authority.

(8)(a) The Authority shall justify its enforcement measures in detail and, before taking such measures, shall notify the entities concerned of its preliminary findings, without prejudice to the provisions of article 21.

(b) The Authority shall also provide a reasonable period of time for interested entities to submit comments, except in duly justified cases where taking immediate action to prevent or address incidents would otherwise be prevented.

Machine Translated by Google

(9) The Authority under this Law shall inform the relevant competent authority in the Republic for the resilience of critical entities when exercising its supervisory and enforcement powers with the aim of ensuring the compliance of an entity identified as a critical entity by the competent authority for the resilience of critical entities with the obligations of this Law, and where appropriate, the competent authority in the Republic may request the Authority to exercise its supervisory and enforcement powers in relation to an entity identified as a critical entity under Directive (EU) 2022/2557.

(10) The Authority shall cooperate with the competent authorities of the Republic pursuant to Regulation (EU) 2022/2554 and, in particular, shall inform the supervisory forum established in accordance with Article 32(1) of Regulation (EU) 2022/2554 when exercising its supervisory and enforcement powers aimed at ensuring the compliance of a key entity designated as a critical third party ICT service provider in accordance with Article 31 of Regulation (EU) 2022/2554 with the obligations of the provisions of this Law:

It is understood that the Authority may be informed of the designation of critical third-party ICT service providers designated in the Republic pursuant to paragraph 9 of article 31 of Regulation (EU) 2022/2554.

Measure supervision and enforcement important entities.

36B.-(1) The Authority shall take measures, where necessary, through ex post supervisory measures in the event that it is provided with evidence, indications or information that a significant entity is suspected of not complying with the obligations set out in this Law for significant entities, in particular with the provisions of articles 35 and 35B of this Law, and such measures shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

(2) The Authority, in exercising its enforcement powers in relation to significant entities, shall have the power to subject such entities to at least-

(a) on-site inspections and ex post supervision outside the premises, carried out by trained professionals;

(b) targeted security audits carried out by an independent body or competent authority:

It is understood that the targeted security audits referred to in paragraph (b) are based on risk assessments carried out by the Authority or the audited entity or on other available information regarding risks:

It is further understood that the results of each targeted security audit shall be made available to the Authority and the cost of such targeted security audit, which is carried out by an independent body, shall be covered by the audited entity, except in duly justified cases for which the Authority decides otherwise;

(c) security scans based on objective, impartial, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;

(d) requests for information necessary for the ex post evaluation of the cybersecurity risk management measures taken by the

Machine Translated by Google

said entity, including documented cybersecurity policies as well as compliance with the obligation to transmit information to the Authority under the provisions of article 37A;

(e) requests for access to data, documents or information necessary for the performance of its supervisory tasks;

(f) requests for evidence regarding the implementation of cybersecurity policies, such as the results of security audits conducted by an authorized auditor and the corresponding underlying evidence.

(3) The Authority, when exercising its powers in accordance with the provisions of paragraphs (d), (e) or (f) of subsection (2), shall state the purpose of the request and specify the information requested.

(4) The Authority, in exercising its supervisory duties in relationship with significant entities, has the power at least to-

(a) issues warnings regarding violations of the provisions of this Law by the entities in question;

(b) issues binding instructions or a Decision to the entities in question to remedy the identified deficiencies or the violation of the obligations of this Law;

(c) requires the entities in question to cease conduct that violates the provisions of this Law and to refrain from repeating such violating conduct;

(d) requires those entities to ensure that their cybersecurity risk management measures comply with the provisions of Article 35 or to fulfil the notification obligations set out in the provisions of Article 35B, in a specified manner and within a specified period of time;

(e) requires those entities to inform natural or legal persons in relation to whom they provide services or carry out activities that may be affected by a significant cyber threat about the nature of the threat, as well as about any protective or remedial measures that those natural or legal persons can take to address that threat;

(f) requires those entities to implement the recommendations made as a result of a security audit within a reasonable period of time;

(g) requires such entities to disclose aspects of violations of the provisions of this Law in a specified manner;

(or) imposes an administrative fine pursuant to the provisions of article 43A in addition to any of the measures referred to in paragraphs (a) to (g) of this subsection.

(5) Subsections (6), (7) and (8) of section 36A shall apply mutatis mutandis to the supervisory and enforcement measures provided for in this section for significant entities.

(6) The Authority shall cooperate with the competent authorities of the Republic pursuant to Regulation (EU) 2022/2554 and in particular inform the

Machine Translated by Google

supervisory forum established under the provisions of paragraph 1 of Article 32 of Regulation (EU) 2022/2554 in the exercise of its supervisory and enforcement powers aimed at ensuring the compliance of a significant entity designated as a critical third party ICT service provider, under the provisions of Article 31 of Regulation (EU) 2022/2554, with the obligations of the provisions of this Law:

It is understood that the Authority may be informed of the designation of critical third-party ICT service providers designated in the Republic pursuant to the provisions of article 31, paragraph 9) of Regulation (EU) 2022/2554.".

The main one law is modified with the replacement of the title of Part Eleventh.

37. The principal law is amended by replacing the title of Part Eleven as follows:

"ENTITY REGISTRY AND DOMAIN NAME REGISTRATION DATABASE".

Amendment the basic law with the deletion of article 37.

38. The basic law is amended by deleting article 37.

Amendment the basic law with the addition of the new article 37A.

39. The basic law is amended by adding, immediately after article 37, the following new article:

“Entity Registry.

37A.-(1) The Authority may submit a request to ENISA for access to the register maintained by ENISA pursuant to the provisions of paragraph 1 of article 27 of Directive (EU) 2022/2555.

(2) The Authority, in the context of implementing subsection (4), requires DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content distribution network providers, managed service providers, managed security service providers, as well as online marketplace providers, online search engine providers or social networking service platforms, to submit the following information:

(a) The name of the entity;

(b) the relevant sector, sub-sector and entity type referred to in the Annexes I and II, as appropriate; Annex I. Annex II.

(c) the address of the entity's main establishment and its other legal establishments in the Republic or in another EU Member State or, if it is not established within the territory of the EU, the address of its representative designated pursuant to the provisions of subsection (3) of article 39;

Machine Translated by Google

(d) up-to-date contact details, including email addresses and telephone numbers, of the entity and, where applicable, of its representative designated in accordance with subsection (3) of section 39;

(e) the other Member States in which the entity provides services; and

(f) the IP ranges of the entity.

(3) The entities referred to in the provisions of subsection (2) shall notify the Authority of any changes to the information submitted pursuant to subsection (2) without delay and, in any case, within three (3) months from the date of the change.

(4) Upon receipt of the information referred to in subsections (2) and (3), except for the information referred to in paragraph (f) of subsection (2), the Authority as a single point of contact shall transmit it to ENISA without undue delay.

(5) Where applicable, the information referred to in subsections (2) and (3) shall be submitted through the national mechanism referred to in subsection (4) of article 27.".

Amendment the basic law with the deletion of article 38.

40. The basic law is amended by deleting article 38.

Amendment the basic law with the addition of the new article 38A.

41. The basic law is amended by adding, immediately after article 38, the following new article:

"Base data registration names sector.

38A.-(1) For the purposes of contributing to the security, stability and resilience of the DNS, the Authority requires TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence, in accordance with the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data Law and Regulation (EU) 2016/679.

(2)(a) For the purposes of subsection (1) the Authority requires that the domain name registration database contain the necessary information for the identification and communication with the domain name holders and the contact points that manage the domain names under the TLDs.

(b) This information includes-

(a) the domain name;

(b) the date of registration;

(c) the name, contact email address and telephone number of the registrant; and

(d) the contact email address and telephone number of the point of contact that

Machine Translated by Google

manages the domain name in case they differ from those of the registrant.

(3)(a) The Authority shall require TLD name registries and entities providing domain name registration services to have policies, including verification procedures, to ensure that the databases referred to in the provisions of subsection (1) contain accurate and complete information.

(b) The Authority requires that such policies and procedures be made public.

(4) The Authority shall require TLD registries and entities providing domain name registration services to make publicly available, promptly after the registration of a domain name, domain name registration data that is not personal data.

(5)(a) The Authority requires TLD registries and entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly justified requests from legitimate access seekers, in accordance with the Law on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data and Regulation (EU) 2016/679.

(b) The Authority requires TLD name registries and entities providing domain name registration services to respond without undue delay and in any event within seventy-two (72) hours of receipt of any access requests.

(c) The Authority requires that the policies and procedures for the disclosure of such data be made public.

(6) Compliance with the obligations set out in subsections (1) to (5) shall not result in duplication of the collection of domain name registration data and, for this purpose, TLD registries and entities providing domain name registration services shall cooperate with each other.'.

Amendment the basic law with the replacement of article 39.

42. Article 39 is replaced by the following article:

"Jurisdiction and territoriality.

39.-(1) Entities falling within the scope of this Law are deemed to fall within the jurisdiction of the Republic, unless they are:

(a) providers of public electronic communications networks or providers of publicly available electronic communications services, which are deemed to fall under the jurisdiction of the Member State in which they provide their services;

(b) DNS service providers, TLD registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines or social networking service platforms, which are deemed to fall under the jurisdiction of

Machine Translated by Google

a Member State in which they have their main establishment in the Union in accordance with subparagraph (2);

(c) public administration entities, which are considered to fall under the jurisdiction of the Member State that has established them.

(2)(a) For the purposes of this Law, an entity referred to in paragraph (b) of subsection (1) shall be deemed to have its main establishment in the Union in the Member State in which decisions relating to risk management measures in the field of cybersecurity are mainly taken.

(b) Where that Member State cannot be determined or where such decisions are not taken in the Union, the main establishment shall be deemed to be located in the Member State in which the cybersecurity operations are conducted.

(c) Where the Member State in question cannot be determined, the main establishment shall be deemed to be located in the Member State in which the entity in question has the establishment with the largest number of employees in the Union.

(3)(a) In the event that an entity referred to in paragraph (b) of subsection (1) is not established in the Republic or in another Member State, but offers services within the Union, it shall appoint a representative in the Union, who shall be established in one of the Member States in which the services are offered.

(b) Such an entity is deemed to be subject to the jurisdiction of Member State in which the representative is established.

(c) In the absence of a representative in the Union designated in accordance with this subsection, the Republic and any other Member State in which the entity provides services may initiate legal proceedings against the entity for breach of the obligations of the provisions of this Law.

(4) The appointment of a representative by an entity referred to in paragraph (b) of subsection (1) does not prejudice legal proceedings that may be initiated against the entity itself.

(5) When the Authority receives a request for mutual assistance in relation to an entity referred to in subsection (1), it may, within the limits of such request, take appropriate supervisory and enforcement measures in relation to the entity concerned which provides services or operates the network and information system in the territory of the Republic.”.

Amendment the basic law with the replacement of the title of Part Twelfth.

43. The basic law is amended by replacing the title of Part Twelve as follows:

"PROVIDERS OF ELECTRONIC COMMUNICATIONS NETWORKS AND/OR SERVICES".

Amendment of article 40 the basic law.

44. Article 40 of the basic law is amended as follows:

(a) By replacing the side title with the following new side title:

"Providers of electronic communications networks and/or services.";

(b) by deleting subsections (1), (2), (3), (4), (5), (7), (8), (9), (10), (12) and (13);

Machine Translated by Google

(c) by replacing subsection (11) with the following subsection:

"(11) In the event that it is established that there is a risk of breach of the security of the network and/or electronic communications services due to the use of the service and/or in the event that it is established that there is a risk of breach of the security of the network of a key and/or important entity, the Authority may request the providers of networks and/or electronic communications services to take measures, including temporary and/or necessary measures, such as the interruption of the service and/or the interruption of access to Internet domain names and/or the interruption of access to IP addresses (Internet
Protocol addresses) in case they are used for cyberattack purposes:

It is understood that the Authority, in the event that the risk referred to in this paragraph ceases to exist or changes, may decide, as the case may be, to lift the temporary and/or necessary measures or to amend these measures.".

Amendment the basic law with the replacement of the title of Part Tenth Third.

45. The principal law is amended by replacing the title of Part Ten Third with the following title:

"STANDARDIZATION, VOLUNTARY NOTIFICATION AND RADIO EQUIPMENT".

Amendment the basic law with the replacement of article 41.

46. Article 41 of the basic law is replaced by the following article:

"Standardization.

41.-(1) The Authority, in order to promote the convergent application of subsections (1) and (2) of article 35, without imposing or favoring the use of a specific type of technology, encourages the use of European and accepted standards and specifications related to the security of network and information systems.

(2) The Authority, in the context of implementing subsection (1), shall take into account any advice and guidelines issued by the ENISA pursuant to the provisions of paragraph 2 of Article 25 of Directive (EU) 2022/2555.".

Amendment the basic law with the addition of the new article 41A.

47. The basic law is amended by adding, immediately after article 41, the following new article:

"Use of European systems certification of cybersecurity.

41A.-(1)(a) In order to demonstrate compliance with the specific requirements of article 35, the Authority may require key and significant entities to use specific ICT products, ICT services and ICT processes, developed by the key or significant entity or procured from third parties, and certified under European cybersecurity certification schemes established in accordance with article 49 of Regulation (EU) 2019/881.

(b) Furthermore, the Authority encourages key and significant entities to use approved trust services.

(2) The Authority shall implement the delegated acts adopted by the Commission pursuant to paragraph 2 of Article 24 of Directive (EU) 2022/2555.".

Machine Translated by Google

Amendment the basic law with the replacement of article 42.

48. Article 42 of the basic law is replaced by the following article:

"Voluntary" notification.

42.-(1) The Authority shall ensure that, in addition to the notification obligation provided for in section 35B, notifications may be submitted to the Authority, on a voluntary basis, by-

(a) key and significant entities regarding incidents, cyber threats and near misses; and

(b) entities other than those referred to in paragraph (a), regardless of whether they fall within the scope of this Law, with regard to significant incidents, cyber threats and near misses.

(2) The Authority shall process the notifications referred to in subsection (1) in accordance with the procedure provided for in the provisions of article 35B, only if such processing does not constitute a disproportionate or unnecessary burden for the Authority.

(3) The Authority may prioritize the processing of mandatory over voluntary notifications.

(4) Where necessary, the Authority, as a single point of contact, shall provide information on the notifications it receives in accordance with this article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity.

(5) Without prejudice to the prevention, investigation and prosecution of criminal offences, voluntary notification shall not impose any additional obligations on the notifying entity which it would not have been subject to if it had not submitted the notification.".

Amendment the basic law with the addition of the new article 42A.

49. The basic law is amended by adding, immediately after article 42, the following following new article:

"Radio equipment.

42A.-(1) The Authority shall ensure that radio equipment of certain categories or classes is manufactured in such a way as to meet the essential requirements specified by the Commission from time to time, and in particular that-

(a) does not harm the network, nor does its operation abuse network resources resulting in unacceptable degradation of service;

(b) incorporates safeguards to ensure the protection of personal data and the privacy of users and the subscriber;

(c) supports certain features that ensure protection against fraud;

(d) supports certain functions to ensure that the installation of software on radio equipment is only possible when the compliance of the combination of radio equipment and software has been demonstrated.

Machine Translated by Google

(2)(a) The Authority shall determine, by its relevant Decision, the requirements that radio equipment must meet in order to be placed on the Cyprus market, put into operation and used, other parameters and procedures for assessing its conformity, as well as the criteria and procedure for approving notified bodies and market surveillance, including the power of seizure;

(b) The Authority shall issue any Decisions necessary to safeguard radio equipment and ensure compliance with the provisions of this Law.

(3)(a) In the event that radio equipment presents a risk to health, safety of persons, security of networks, information and information systems or other issues of protection of the public interest, an assessment is carried out and all necessary measures are taken to bring the equipment into compliance or eliminate the risk and the Authority determines in its relevant Decision, the assessment procedure as well as the measures that may be taken.

(b) The Authority shall notify the Commission of any decision it has taken regarding radio equipment that does not comply with the relevant provisions of the applicable legislation.".

Amendment of article 43 the basic law.

50. Article 43 of the basic law is amended as follows:

(a) By replacing in subsection (1) the word "In", (first line), with the phrase "Without prejudice to article 43A, in";

(b) by replacing subsection (3) with the following subsection:

"(3) The Authority may issue Decisions, for the procedure for imposing an administrative fine and/or other administrative sanctions in relation to non-compliance with the provisions of this Law and/or Decisions and/or Regulations of the European Union, within the meaning assigned to the terms by the Implementation of Community Regulations and Community Decisions Law of 2007 and determine by its Decision the amount of these fines and sanctions and the procedure for imposing them.";

(c) by substituting in subsection (4) the words "the Commissioner" (first line), with the words "the Authority"; and

(d) by adding, in subsection (5) immediately after the phrase "by registered letter" (second and third lines), the phrase "and/or electronically, in a manner determined by the Authority,".

Amendment the basic law with the addition of the new article 43A.

51. The basic law is amended by adding, immediately after article 43, the following following new article:

"Enforcement administrative fines to basic and important entities.

43A.-(1) The administrative fines imposed under this article, on key and significant entities in relation to the infringement of the provisions of this Law, shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

(2) Administrative fines are imposed in addition to any of the measures referred to in paragraphs (a) to (h) of subsection (4) of article 36A, in subsection (5) of article 36A and in paragraphs (a) to (g) of subsection (4) of article 36B.

Machine Translated by Google

(3) The Authority, when making a decision regarding the imposition of an administrative fine and deciding on its amount in each individual case, shall take due account, at a minimum, of the provisions of subsection (7) of article 36A.

(4) In the event of a violation of Articles 35 and 35B of this Law, the main entities shall be subject, in accordance with subsections (2) and (3), to administrative fines of a maximum amount of at least ten million euros (€10,000,000) or a maximum amount of at least 2% of the total worldwide annual turnover of the undertaking to which the main entity belongs in the preceding financial year, whichever is higher.

(5) In the event of a breach of Articles 35 and 35B of this Law, significant entities shall be subject, in accordance with subsections (2) and (3), to administrative fines of a maximum amount of at least seven million euros (€7,000,000) or a maximum amount of at least 1.4% of the total worldwide annual turnover of the undertaking to which the significant entity belongs in the preceding financial year, whichever is higher.

(6) The Authority may, by its Decision, provide for the imposition of other administrative sanctions, in order to oblige a key or significant entity to cease a violation of the provisions of this Law in accordance with its previous Decision.”.

Amendment of article 44 the basic law.

52. Article 44 of the basic law is amended as follows:

(a) By amending subsection (1) as follows:

(i) By replacing the phrase “Operator of essential services and/or critical information infrastructure operator which” (first and second lines), with the phrase “Essential and/or significant entity which”;

(ii) by replacing the phrase "he is guilty" (third line), with the phrase "she is guilty";

(iii) by replacing the words "condemnation of" (fourth line), with the words of "condemnation"; and

(iv) by deleting the word "the" (fifth line);

(b) by deleting subsections (2) and (4); and

(c) by amending subsection (3) as follows:

(i) by replacing the phrase “Operator of essential services and/or critical information infrastructure operator which” (first and second lines), with the phrase “Essential and/or significant entity which”;

(ii) by replacing the phrase “he is guilty” (fourth line), with the phrase “she is guilty”; and

(iii) by replacing the words "condemnation of" (fourth line), with the words of "condemnation".

Amendment the basic law with the addition of the new article 44A.

53. The basic law is amended by adding immediately after article 44, the following: following new article:

Machine Translated by Google

"Violations" where entail infringement data personnel character.

44A.-(1) In the event that the Authority becomes aware, in the context of supervision or enforcement, that the breach by a key or significant entity of the obligations set out in the provisions of articles 35 and 35B may result in a personal data breach, as defined in point 12 of article 4 of Regulation (EU) 2016/679, which must be notified in accordance with article 33 of that Regulation, it shall inform without undue delay the supervisory authorities referred to in article 55 or 56 of that Regulation.

(2)(a) Where the supervisory authorities referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine in accordance with Article 58(2)(i) of that Regulation, the Authority shall not impose an administrative fine in accordance with the provisions of Article 43A for the infringement referred to in paragraph (1) and which results from the same conduct that was the subject of the administrative fine in accordance with Article 58(2)(i) of Regulation (EU) 2016/679.

(b) The Authority may, however, apply the enforcement measures referred to in paragraphs (a) to (h) of subsection (4) of article 36A, in subsection (5) of article 36A and in paragraphs (a) to (g) of subsection (4) of article 36B.

(3) In the event that the supervisory authority competent under Regulation (EU) 2016/679 is established in a Member State other than the Authority, the Authority shall inform the Commissioner for Personal Data Protection of the possible breach of the data referred to in subsection (1).

Amendment of article 47 the basic law.

54. Article 47 of the basic law is amended by replacing subsection (2) with the following subsection:

"(2)(a) The budget shall be submitted by the Commissioner, through the Deputy Minister, for approval to the Minister of Finance, who shall submit it to the Council of Ministers.

(b) After the budget is approved by the Council of Ministers, it is submitted to the House of Representatives for approval in accordance with the provisions of article 104 of the Fiscal Responsibility and Fiscal Framework Law.".

Amendment of article 55 the basic law.

55. Article 55 of the basic law is amended by adding, immediately after subsection (2), the following new subsections:

"(3) Decisions or Regulations issued under the Network and Information Systems Security Law of 2020 shall remain in force until their repeal or replacement by Decisions, Regulations issued under the provisions of this Law or in the context of fulfilling Union obligations, as the case may be.

(4) With the entry into force of a law, according to the provisions of which, the structure, administration, operation, personnel matters, financial management and budget of the Authority will be amended with the unification of the Authority with OCECPR, and specifically articles 4 to 14, paragraphs (b) to (f) of subsection (2) of article 45, article 47, article 50 and article 53 of the Network and Information Systems Security Law are expected to be amended or repealed accordingly.

Amendment the basic law with the addition of Annexes I and II.

56. The basic law is amended by adding, immediately after article 56, the following: Annexes I and II which are included in the Table of this Law.

Machine Translated by Google

Inception of power of the present Law.

57.-(1) Subject to subsection (2), this Law shall come into force on date of its publication in the Official Gazette of the Republic.

(2) The provisions of article 7 of this Law shall come into force on a date determined by the Council of Ministers by notification thereof, which shall be published in the Official Gazette of the Republic.

Machine Translated by Google

PANEL

(Article 56)

ANNEX I

(Articles 2A and 27)

HIGH CRITICAL AREAS

		Subdomain	Entity Type
1.	Energy Sector	a) Electricity	— Electricity undertakings, as defined in accordance with the provisions of the Electricity Market Regulation Law, which carry out the activity of "supply", as defined in accordance with the provisions of the same Law
			— Distribution system operators as defined in accordance with the provisions of the Regulation of the Electricity Market Law
			— Cyprus Transmission System Operator, as defined in accordance with the provisions of the Electricity Market Regulation Law — Producers as defined in accordance with the provisions of the Electricity Market Regulation Law Law
			— Designated electricity market operators has the meaning assigned to this term in Article 2(8) of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market in electricity.
			— Market participants, has the meaning assigned to this term in Article 2 point (25) of Regulation (EU) 2019/943, who provide energy aggregation, demand response or storage services, as defined in accordance with the provisions of the Electricity Market Regulation Law
			— Recharging point operators responsible for the management and operation of a recharging point, which provides a recharging service to end-users, including on behalf of and on behalf of a mobility service provider
		b) District heating and cooling	— District heating or district cooling operators, as defined in accordance with the provisions of the Electricity Market Regulation Law
		c) Oil	— Oil pipeline operators
			— Managers of oil production, refining and processing facilities, oil storage and transportation
			— Central stockholding entities, as defined in accordance with the provisions of the Petroleum Reserve Conservation Law
		d) Gas	— Supply undertakings as defined in accordance with the provisions of the Market Regulation Act Natural Gas Law
			— Distribution system operators as defined in accordance with the provisions of the Regulation of the Electricity Market Law

Machine Translated by Google

			— Transmission system operators as defined in accordance with the provisions of the Regulation of the Natural Gas Market Law — Storage network operators as defined in accordance with the provisions of the Regulation of the Natural Gas Market Law — LNG system operators as defined in accordance with the provisions of the Regulation of Natural Gas Market Law — Natural gas undertakings as defined in accordance with the provisions of the Regulation of Natural Gas Market Law — Natural gas refining and processing facility operators
		e) Hydrogen	— Hydrogen production, storage and transportation operators
2.	Transportation	a) Aerial	— Air carriers has the meaning assigned to that term in Article 3 point (4) of Regulation (EC) No 300/2008, used for commercial purposes — Airport managing bodies, as defined in accordance with the provisions of the Civil Aviation Law and airports as defined in accordance with the provisions of the Civil Aviation Law, including hub airports listed in Annex II, Section 2 of Regulation (EU) No 1315/2013 of the European Parliament and of the Council, and operators of ancillary facilities located within airports
			— Air traffic management control operators providing air traffic control services as defined in Article 2(1) of Regulation (EC) No 549/2004 of the European Parliament and of the Council
		b) Railways	— Infrastructure managers as defined in Article 3(2) of Directive 2012/34/EU of the European Parliament and of the Council — Railway undertakings, as defined in accordance with the provisions of the Railway Undertaking Licensing Law, including operators of facilities for the provision of services as defined in Article 3 point 12) of Directive 2012/34/EU
		c) Floating	— Inland waterway, maritime and coastal passenger and freight transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council4, not including individual ships used by such companies — Port managing bodies, as defined in accordance with the provisions of the Law on the Enhancement of Port Security, including their port facilities as defined in Article 2 point (11) of Regulation (EC) No. 725/2004, and operators of works and equipment located within ports — Vessel Traffic Service (VTS) operators, as defined in accordance with the provisions of the Merchant Shipping (Community Vessel Monitoring System)

[4] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 1).
p. 6).

Machine Translated by Google

			and Information Regarding Ship Traffic) Law
		d) Roads	— Road authorities, has the meaning assigned to this term in Article 2(12) of Commission Delegated Regulation (EU) 2015/962, responsible for the control of traffic management, with the exception of public bodies for which traffic management or the operation of intelligent transport systems constitutes a non-essential part of their general activity — Intelligent Transport Systems (ITS) operators, as defined in accordance with the provisions of the Law on the Development Framework for Intelligent Transport Systems in the Road Transport Sector and Interfaces with other Modes of Transport
3.	Banks		— Credit institutions has the meaning assigned to this term in Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
4.	Financial market infrastructures		— Trading venue operators, as defined in accordance with the provisions of the Investment Services and Activities and Regulated Markets Law — Central counterparties, has the meaning assigned to this term in Article 2 point 1) of Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories
5.	Health		— Healthcare providers, as defined in accordance with the provisions of the Implementation of Patients' Rights in the Context of Cross-Border Healthcare Law — EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU — Entities carrying out research and development activities on medicinal products, referred to in Article 1(2) of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in Section C Division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered critical during a public health emergency (list of medical devices critical during a public health emergency) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on strengthening the role of the European Medicines Agency in relation to crisis-preparedness and crisis management for medicinal products and medical devices

Machine Translated by Google

6.	Drinking water	Suppliers and distributors of water for human consumption as provided for under the provisions of the Water Quality for Human Consumption Law, excluding distributors for whom the distribution of water for human consumption constitutes an insignificant part of their general activity of distributing other products and goods
7.	Effluent	Enterprises for the collection, disposal or treatment of urban, domestic or industrial wastewater defined in accordance with the provisions of the Integrated Water Management Law, excluding enterprises for which the collection, disposal or treatment of urban, domestic or industrial wastewater constitutes an insignificant part of their general activity.
8.	Digital infrastructures	— Internet exchange point providers — Domain Name System (DNS) service providers, excluding administrators of root name servers — Top-level domain name (TLD) registries — Cloud computing service providers — Data center service providers — Content distribution network providers — Trust service providers; — Providers of public electronic communications networks — Providers of publicly available electronic communications services
9.	ICT service management (business-to-business)	— Managed service providers — Managed security service providers
10.	Public administration entities	— Central government public administration entities — Public administration entities of the broader public sector
11.	Space	Operators of terrestrial infrastructure, owned, managed and operated by Member States or private entities, which support the provision of space services, excluding providers of public electronic communications networks

Machine Translated by Google

ANNEX II

(Articles 2A and 27)

OTHER CRITICAL AREAS

	Sector	Subdomain	Entity Type
1.	Postal and courier services		Postal service providers as defined in accordance with the provisions of the Regulation of Electronic and Postal Services Law, including courier service providers Communications
2.	Waste management		Waste management enterprises as defined in accordance with the provisions of the Waste Law, with the exception of enterprises for which waste management is not the main economic activity
3.	Manufacture, production and distribution of chemical products		Undertakings involved in the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3 points (9) and (14) of Regulation (EC) No 1907/2006 of the European Parliament and of the Council, and undertakings producing articles, as defined in Article 3 point (3) of that Regulation, from substances or mixtures
4.	Food production, and processing and distribution		Food businesses, as defined in Article 3 point (2) of Regulation (EC) No. 178/2002 of the European Parliament and of the Council, which are active in wholesale distribution and industrial production and processing
5.	Construction sector	a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices as defined in point (1) of Article 2 of Regulation (EU) 2017/745 of the European Parliament and of the Council, and entities manufacturing in vitro diagnostic medical devices as defined in point (2) of Article 2 of Regulation (EU) 2017/746 of the European Parliament and of the Council, with the exception of entities manufacturing medical devices referred to in the fifth indent of point 5 of Annex I to this Directive
		b) Manufacturing of computer, electronic and optical products	Enterprises carrying out economic activities listed in sector C, division 26 of the NACE rev. 2
		c) Construction of electrical equipment	Enterprises carrying out economic activities listed in sector C, division 27 of the NACE rev. 2

Machine Translated by Google

		d)Manufacture of machinery and equipment n.e.c.	Enterprises carrying out economic activities listed in sector C, division 28 of the NACE rev. 2
		e) Manufacture of motor vehicles, trailers and semi-trailers	Enterprises carrying out economic activities listed in sector C, division 29 of the NACE rev. 2
		f) Manufacture of other transport equipment	Enterprises carrying out economic activities listed in sector C, division 30 of the NACE rev. 2
6.	Digital providers		— Online shopping providers — Online search engine providers — Social media platform providers
7.	Research		Research organizations