89(I)/2020

OFFICIAL GAZETTE

OF THE REPUBLIC OF CYPRUS

ANNEX I

LEGISLATION – PART ONE

Number 4770 Wednesday, 12 August 2020

The Security of Networks and Information Systems Law of 2020 is hereby promulgated in the Official Gazette of the Republic of Cyprus pursuant to Article 52 of the Constitution.

Number 89(I) of 2020

SECURITY OF NETWORKS AND INFORMATION SYSTEMS LAW OF 2020

2 of 60(I) of 2025. Preamble.

(a) For the purposes of harmonisation with the European Union act entitled:

Official Journal 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 on 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 2 Directive)'; and

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

'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'.

The House of Representatives has decided as follows:

Short title. 60(I) of 2025.

1. This Law shall be referred to as the Security of Networks and Information Systems Laws of 2020 and 2025.

PART ONE
GENERAL – INTERPRETATIVE PROVISIONS

Exemptions from the scope of application. Official Journal of the EU: L 257, 28.8.2014, p. 73.

2.-(1) Deleted by 3(a) of 60(I) of 2025.

3(b) of 60(I) of 2025.

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

(b) Without prejudice to the provisions of paragraph (4), this Law shall not apply to public administration entities which carry out their activities in the areas of national security, public security, defence or law enforcement, including the

prevention, investigation and prosecution of criminal offences.

3(c) of 60(I) of 2025. 91(I) of 2014 105(I) of 2014. 147(I) of 2015. Official Journal of the EU: L 119, 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. Official Gazette Annex Three (I): 20.1.2012.

(3) This Law shall apply without prejudice to Regulation (EU) 2016/679, the Law on the Regulation of Electronic Communications and Postal Services, the Law on Electronic Communications, the Law on the Prevention and Combating of Sexual Abuse, Sexual Exploitation of Children and Child Pornography, the Law on Attacks against Information Systems and the 'Identification and designation of the European critical infrastructure and assessment of the need to improve their protection' regulations.

3(d) of 60(I) of 2025

(4)(a) The Authority may, in application of the provisions of Article 27(7), exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in Article 2(2), point (b), from the obligations laid down in Article 35 or 35B of this Law with regard to those activities or services.

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

3(d) of 60(I) of 2025

(5) This law shall not apply to the security of networks and information systems and to the infrastructure and facilities of the Cypriot Intelligence Service.

4 of 60(I) of 2025. Scope. Official Journal of the EU: L 124, 20.5.2003, p. 36. Annex I. Annex II.

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

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

Annex I. Annex II.

(2) Regardless of their size, this Law also applies to entities of the types referred to in Annex I or II, where:

(a) services are provided by:

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

(ii)trust service providers; and

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

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

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

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

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

(f) the entity is a public administration entity:

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

(ii) of the wider public sector, which, following a risk-based assessment, provides services, the disruption of which could have a significant impact on critical societal or economic activities.

(3) Regardless of their size, this Law applies to entities identified as critical entities by the competent authority for critical entity resilience.

(4) Regardless of their size, this Law applies to entities providing domain name registration services.

(4) Regardless of their size, this Law applies to entities providing domain name registration services.

(5) Subject to the provisions of Article 27(7), this Law applies to public administration entities at local level and may apply to education institutions, in particular where they carry out critical research activities.

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

(6) Article 2(2)(b) and Article 2(4) shall not apply where an entity acts as a trust service provider.

(7) The obligations laid down in this Law shall not entail the supply of any information which, if disclosed, would be incompatible with the Republic's essential national security, public security or defence interests.

(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) 2016/679, in particular such processing shall rely on Article 6 of that Regulation:

The processing of personal data pursuant to this Law by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, the Law on the Regulation of Electronic Communications and Postal Services and the Law on Electronic Communications.

(9) Where sector-specific EU legal acts require essential or important 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 laid down in Articles 36, 36A and 36B, shall not apply to such entities and where sector-specific EU legal acts do not cover all entities in a specific sector falling within the scope of this Law, the relevant provisions of this Law shall continue to apply to the entities not covered by those sector-specific EU legal acts.

(10) The requirements referred to in paragraph 9 of this Article shall be considered to be equivalent in effect to the obligations laid down in this Law where:

(a) the cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 35(1) and (2); or

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

Definitions.

3.-(1) For the purposes of this Law, unless the context indicates otherwise:

'representative' is deleted by 5(b)(i) of 60(I) of 2025.

'Authority' means the Digital Security Authority;

5(c) of 60(I) of 2025.

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

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

'Deputy Commissioner' means the Deputy Commissioner for Communications, appointed under the provisions of Article 5(2) of the Law on the Regulation of Electronic Communications and Postal Services, who advises and assists the Commissioner in the exercise of their functions, powers and duties provided by this Law and performs any other duties assigned to them under this Law;

104(I) of 2016
112(I) of 2016
76(I) of 2017.

5(d) of 60(I) of 2025. **'the Office' or 'OCECPR'** means the Office of the Commissioner for Electronic Communications and Postal Regulation established under the provisions of the Law on the Regulation of Electronic Communications and Postal Services;

'Republic' means the Republic of Cyprus;

5(a) of 60(I) of 2025. **'information and communication technology process'** or 'ICT process' under Regulation (EU) 2019/881;

5(a) of 60(I) of 2025. **'public electronic communications network'** shall have the meaning attributed to this term in Article 5 of the Law on Electronic Communications;

5(a) of 60(I) of 2025. **'network'** means the network of national coordination centres;

5(a) of 60(I) of 2025. **'content delivery network'** means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

5(a) of 60(I) of 2025. **'CSIRT network'** means the network established and operating pursuant to Article 15 of Directive (EU) 2022/2555;

5(e) of 60(I) of 2025. **'network and information system'** means:

(a) an electronic communications network as defined in Article 4(1) of the Law on the Regulation of Electronic Communications and Postal Services; or

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

5(a) of 60(I) of 2025. Official Journal of the EU: L 257, 28.8.2014, p. 73. **'qualified trust service'** shall have the meaning given to this term in Article 3(17) of Regulation (EU) No 910/2014;

5(a) of 60(I) of 2025. **'qualified trust service provider'** shall have the meaning given to this term in Article 3(20) of Regulation (EU) No 910/2014;

5(f) of 60(I) of 2025. **'national cybersecurity strategy'** means a coherent framework of the Republic that provides strategic objectives and priorities in the area of cybersecurity and the governance to achieve them within the Republic;

'national CSIRT' means a national entity that directly responds to incidents relating to the security of network and information systems;

5(a) of 60(I) of 2025. **'representative'** means a natural person or legal entity established either in the Republic or in other Member States, explicitly appointed to act on behalf of a DNS

service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Republic or in another Member State, which may be addressed by the Authority or the national CSIRT in the place of the entity itself with regard to the obligations of that entity under this Law;

5(a) of 60(I) of 2025. **'single point of contact'** shall have the meaning given to this term pursuant to Article 17(c) of this Law;

5(g) of Law 60(I) of 2025. **'online marketplace'** means a service using software, including a website, part of a website or an application, operated by or on behalf of a trader, which allows consumers to enter into remote contracts with other traders or consumers using software, including a website, part of a website or an application, operated by or on behalf of a trader;

5(h) of Law 60(I) of 2025. **'online search engine'** shall have the meaning given to this term in Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services;

'Commissioner' means the Commissioner for Communications appointed pursuant to Article 5(1) of the Law on the Regulation of Electronic Communications and Postal Services;

'Commission' means the Commission of the European Union;

'ENISA' means the European Union Agency for Cybersecurity;

5(a) of 60(I) of 2025. **'EU-CyCLONe'** means the European Cyber Crisis Liaison Organisation Network;

5(a) of 60(I) of 2025. **'vulnerability'** means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyberthreat;

5(a) of 60(I) of 2025. **'research activity'** means an applied research or experimental development conducted in accordance with the Organisation for Economic Co-operation and Development's Frascati Manual 2015, entitled 'Guidelines for Collecting and Reporting Data on Research and Experimental Development', with a view to exploiting the results for commercial purposes, such as the manufacturing or development of a product or process, the provision of a service, or the marketing thereof;

5(a) of 60(I) of 2025. Annex II. **'research organisation'** means an entity listed in Annex II which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions;

5(a) of 60(I) of 2025. **'general public sector'** means independent services not included in the budget of the Republic, legal entities governed by public law and public-law entities that are not part of central government;

5(a) of 60(I) of 2025. **'day'** means a calendar day, unless otherwise specified in this Law;

Official Journal of the EU: L 316, 14.11.2012, p. 12.

'Regulation (EU) No 1025/2012' means Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council;

Official Journal of the EU: L 119, 4.5.2016, p. 1.

'Regulation (EU) 2016/679' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

5(a) of 60(I) of 2025. Official Journal of the EU: L 151, 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 information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), as amended or replaced;

5(a) of 60(I) of 2025. Official Journal of the EU: L 333, 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 for 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;

'Central Bank' means the Central Bank of Cyprus;

5(i) of 60(I) of 2025.

'risk' means the potential for loss or disruption caused by an incident, expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

5(a) of 60(I) of 2025.

'class of radio equipment' means a class which identifies specific categories of radio equipment considered similar under the provisions of this Law and those radio contacts for which the radio equipment is designed;

5(a) of 60(I) of 2025.

'State body' or 'central government' means ministries, deputy ministries, their departments, agencies, their directorates, bodies of constitutional powers and services, independent services and essential and/or important entities included in the budget of the Republic;

'critical infrastructure' Deleted by 5(b)(ii) of 60(I) of 2025.

'critical information infrastructure' Deleted by 5(b)(iv) of 60(I) of 2025.

5(a) of 60(I) of 2025.

'cybersecurity' shall have the meaning given to this term in Article 2(1) of Regulation (EU) 2019/881;

5(a) of 60(I) of 2025.

'cyberthreat' shall have the meaning given to this term in Article 2(8) of Regulation (EU) 2019/881;

5(a) of 60(I) of 2025. 75(I) of 2016 and 14(I) of 2023.

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

5(a) of 60(I) of 2025.

'top-level domain name registry' or 'TLD name registry' means an entity which has been delegated a specific TLD and is responsible for administering 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 across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

'top-level domain name registry' Deleted by 5(b) of 60(I) of 2025.

5(a) of 60(I) of 2025. Official Journal of the EU: L 153, 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;

'Directive (EU) 2016/1148' Deleted by 5(b)(iii) of 60(I) of 2025.

5(a) of 60(I) of 2025. Official Journal of the EU: L 333, 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 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), as amended or replaced;

5(a) of 60(I) of 2025.

'Cooperation Group' means a cooperation group established under Article 14 of Directive (EU) 2022/2555;

5(a) of 60(I) of 2025.

'public administration entity' means an entity, not including the judiciary, the House of Representatives or the Central Bank of Cyprus, which complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and is not of an industrial or commercial nature;

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

(c) it is financed for the most part by central government or other bodies governed by public law, is subject to management supervision by those authorities or bodies or has an administrative, managerial 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) it has the power to address to natural persons' or legal entities' administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;

5(a) of 60(I) of 2025.

'entity providing domain name registration services' means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;

5(a) of 60(I) of 2025. **'entity'** means a natural person or legal entity created and recognised as such under the national law of the place where it was established, which may, acting under its own name, exercise rights and be subject to obligations;

5(a) of 60(I) of 2025. **'near miss'** means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or did not materialise;

5(a) of 60(I) of 2025. **'provider'** means a person who provides or is authorised to provide electronic communications networks and/or services and/or associated facilities to the public;

5(a) of 60(I) of 2025. **'managed service provider'** means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely;

5(a) of 60(I) of 2025. **'managed security service provider'** means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

'electronic communications network provider' means a person authorised by the Commissioner to provide a public electronic communications network under the Law on the Regulation of Electronic Communications and Postal Services;

5(a) of 60(I) of 2025. **'DNS service provider'** means an entity that provides:

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

(b) authoritative domain name resolution services for third-party use, with the exception of root name servers;

5(a) of 60(I) of 2025. **'trust service provider'** means a trust service provider as defined in Article 3(19) of Regulation (EU) No 910/2014;

'electronic communications service provider' means a person authorised by the Commissioner to provide electronic communications services available to the public under the Law on the Regulation of Electronic Communications and Postal Services;

'domain name system service provider' means an entity that provides internet-based domain name system services;

'digital service provider' is deleted by 5(b)(vi) of 60(I)/2025.

5(a) of 60(I) of 2025. **'incident'** means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

5(a) of 60(I) of 2025. **'large-scale cybersecurity incident'** means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a

significant impact on at least two Member States;

5(a) of 60(I) of 2025. **'social networking services platform'** means a platform that enables end users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;

'specification' Deleted by 5(b)(vii) of 60(I) of 2025.

5(a) of 60(I) of 2025. **'ICT product'** shall have the meaning given to this term in Article 2(12) of Regulation (EU) 2019/881;

'supervisor' means the person holding the hierarchical superior position at the Authority, who is subordinate of the Commissioner;

5(a) of 60(I) of 2025. **'person'** means a main and/or significant entity and any other legal or natural persons or organisations which the Authority considers as a person for the purposes of this Law, based on its competences hereunder;

'standard' means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012;

5(a) of 60(I) of 2025. **'radio equipment'** means an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination;

5(a) of 60(I) of 2025. **'significant cyberthreat'** means a cyberthreat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage;

5(j) of Law 60(I) of 2025. **'internet exchange point' or 'IXP'** means a network facility which enables 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 the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

'event' means any event that has an actual adverse impact on the security of networks and information systems;

'Advisory Committee' shall have the meaning given to this term in Article 32 of the Law on the Regulation of Electronic Communications and Postal Services;

5(a) of 60(I) of 2025. 'Recommendation 2003/361/EC' means the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;

5(k) of 60(I) of 2025. **'domain name system' or 'DNS'** means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those

services and resources;

5(a) of 60(I) of 2025. **'ICT'** means information and communication technology;

5(a) of 60(I) of 2025. **'technical specifications'** shall have the meaning given to this term in Article 2(4) of Regulation (EU) No 1025/2012;

5(a) of 60(I) of 2025. **'trust service'** shall have the meaning given to this term in Article 3(16) of Regulation (EU) No 910/2014;

5(a) of 60(I) of 2025. **'electronic communications service'** means an electronic communications service as defined in Article 2 of the Law on Electronic Communications;

5(a) of 60(I) of 2025. **'data centre service'** means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructure for power distribution and environmental control;

'cloud computing service' Deleted by 5(b)(viii) of 60(I) of 2025.

5(a) of 60(I) of 2025. **'ICT service'** shall have the meaning given to this term in Article 2(13) of Regulation (EU) 2019/881;

5(a) of 60(I) of 2025. **'cloud computing service'** means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

'Deputy Minister' means the Deputy Minister for Research, Innovation and Digital Policy attached to the President.

5(l) of 60(I) of 2025. **'operator of essential services'** means a public or private entity of a type referred to in a decision issued by the Authority;

'critical information infrastructure operator' means an operator managing critical information infrastructure, referred to in a decision of the Authority;

5(a) of 60(I) of 2025. **'incident handling'** means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident;

'event handling' Deleted by 5(e)(ix) of 60(I) of 2025.

5(m) of 60(I) of 2025. **'digital service'** means a service as defined in Article 1(1)(b) of Directive (EU) 2015/1535 of the European

Official Journal of the EU: L 241, 17.9.2015, p. 1. Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, of a type referred to in a decision adopted by the Authority;

(2) Terms used in this Law and not otherwise defined shall have the meaning given to them in the Law on the Regulation of Electronic Communications and Postal

Services.

PART TWO
APPOINTMENT AND DISMISSAL OF A COMMISSIONER AND OF A DEPUTY COMMISSIONER FOR COMMUNICATIONS

Appointment and dismissal of a Commissioner and of a Deputy Commissioner for Communications.

4. For the appointment and dismissal of a Commissioner and of a Deputy Commissioner for Communications, Articles 5 to 7 of the Law on the Regulation of Electronic Communications and Postal Services shall apply regarding the performance of their duties under the provisions of this Law.

Remuneration and obligations of the Commissioner and of the Deputy Commissioner for Communications.

5. Articles 8 and 9 of the Law on the Regulation of Electronic Communications and Postal Services shall apply to the remuneration and obligations of the Commissioner and of the Deputy Commissioner for Communications in general as well as to their obligations after their retirement.

PART THREE
DIGITAL SECURITY AUTHORITY

Competent national authority for the security of network and information systems and cybersecurity. 17(I) of 2018.

6.-(1) The Commissioner who has been appointed as the head of the Authority and as the national authority for the security of networks and information systems and for the coordination of the implementation of the cybersecurity strategy, pursuant to Article 3 of the Security of Networks and Information Systems Law, shall continue to be the head of the Authority and shall have the functions provided for in this Law.

(2)(a) The Commissioner shall be assisted in the exercise of his functions, powers and duties provided in this Law by the Deputy Commissioner, who shall advise and assist the Commissioner in such a way as the Commissioner may decide, and perform any other duties assigned to him or her under this Law.

(b) In the event that the Commissioner is dismissed or resigns, in accordance with Article 6 of the Law on the Regulation of Electronic Communications and Postal Services, or in the event of death, permanent absence or another permanent impediment to the exercise of his or her functions, powers and duties pursuant to the Law on the Regulation of Electronic Communications and Postal Services and/or this Law, the functions, powers and duties assigned to the Commissioner under this Law shall be exercised temporarily by the Deputy Commissioner until another Commissioner is appointed, as provided for in the Law on the Regulation of Electronic Communications and Postal Services.

(c) In the event of a temporary absence, illness, mental or physical incapacity or disability or other temporary impediment that renders the Commissioner incapable of fulfilling his functions, powers and duties under this Law for a short period of time, such functions, powers and duties shall be exercised temporarily by the Deputy Commissioner.

(3) For the exercise of the functions of the Commissioner in accordance with paragraph 1, as head of the national authority for the security of network and information systems and for the coordination of the implementation of the cybersecurity strategy, the Authority established under Article 3(3) of the Security of Networks and Information Systems Law of 2018 as an independent authority with a separate legal personality shall continue to function as the competent national authority for the implementation of the provisions of this Law.

6(a) of 60(I) of 2025.

(4) The Authority shall continue to be staffed, operated and administered under the provisions of the Law on the Regulation of Electronic Communications and Postal Services and the decisions and regulations made pursuant to this Law.

(5) The staff of the Authority shall act in accordance with the orders or instructions of the Commissioner and shall provide the Commissioner and the Deputy Commissioner with every possible facility to fulfil the functions and powers of the Authority under the provisions of this Law.

(6) The Commissioner shall exercise supervision and control over the Authority and its staff.

(7) The Authority shall take all appropriate measures and all necessary actions to ensure that the financial and human resources at its disposal are sufficient to carry out the tasks entrusted to it.

(8) In the performance of its duties, the Authority shall apply the relevant legislation concerning any secret and confidential information it handles.

(9) The national CSIRT, which is part of the Authority in accordance with Article 3(8) of the Security of Networks and Information Systems Law of 2018, shall continue to receive instructions and guidance from the Authority and shall be under its supervision.

6(b) of 60(I) of 2025.

(10) the Commissioner is responsible for advising the Deputy Minister on matters relating to the security of network and information systems, digital security and cybersecurity in the Republic of Cyprus.

Powers of the Authority in relation to the acquisition, disposal and investment of property.

7. The Authority may:

(a) acquire by purchase, exchange, donation or in any other way any immovable or movable property for its housing and operational needs;

7 of 60(I) of 2025.

(a) accept the provision of grants for the purpose of implementing the provisions of this Law, from the Republic, the European Union, an international organisation or from a company or organisation, provided that the latter is not an essential or important entity which has a financial or other interest, directly or indirectly, in the Authority and does not have in any event any involvement in any such essential or important entity;

(c) sell, exchange, lease, assign or dispose in any other way of any movable or immovable property of the Authority and mortgage or encumber such property for its needs;

(d) lease or secure a license to use any immovable or movable property for the housing and operation needs of the Authority;

20(I) of 2014
123(I) of 2016
133(I) of 2016
159(I) of 2017.

(e) make loans which are necessary for the implementation of all the provisions included in points (a), (c) and (d), in compliance with Article 103 of the Fiscal Responsibility and Financial Framework Law;

(f) receive, subject to the provisions of this Article and Article 8, and manage all amounts paid pursuant to this Law or the decisions or regulations made thereunder;

(g) conclude contracts; and

(h) do anything required to fulfil the provisions of this Article.

Fund of the Authority.

8. The Authority shall have a separate fund, in which the following shall be deposited:

(a) all amounts payable and collected by the Authority, provided for under this Law and/or the decisions and/or provisions of the regulations adopted thereunder;

(b) any grant provided to the Authority pursuant to Article 7(b) and any other income received pursuant to this Law;

(c) all revenues derived from the Authority's assets in accordance with Article 7;

(d) all amounts of salaries, emoluments, benefits, pensions, remuneration and hire of services paid by the Republic to the Authority, in accordance with Article 11(1), for payment by the Authority to its members of staff or to persons with whom it has concluded service contracts pursuant to Article 14, as the case may be.

Article 9 will be deleted by 8 of 60(I) of 2025, in accordance with Article 57(2) of 60(I) of 2025.

Staff of the Authority.

9.-(1) For the appointments and promotions of the staff of the Authority, a three-member Board, referred to as the 'Selection and Promotions Council of the Digital Security Authority' ('SPCA'), shall be set up and shall comprise:

(a) the Commissioner, as chair;

the Deputy Commissioner; and

(c) the Chair of the Advisory Committee, appointed pursuant to Article 32(1)(b) of the Law on the Regulation of Electronic Communications and Postal Services. Should the Chair be unavailable, he or she shall be substituted by one of the two members of the Advisory Committee, appointed by the Commissioner.

(2) The members of staff of the Authority shall be appointed by the SPCA either permanently or on contract for a specified period of time in accordance with the relevant procedures laid down in Regulations adopted pursuant to Article 45.

(3) The SPCA may approve increments on the basis of the qualifications, practice and experiences of the person appointed, in proportion to the criteria applicable in the public service, by placing such person at any point on the scale or combined scales provided by the scheme of service for the post.

(4)(a) Regulations adopted pursuant to Article 45 of this Law may prescribe, regulate and provide for procedures and other matters relating to the recruitment, permanence, promotion, terms of service, categories of posts, retirement and retirement benefits for the members of staff of the Authority.

97(I) of 1997
3(I) of 1998
77(I) of 1999
141(I) of 2001
69(I) of 2005
37(I) of 2010
94(I) of 2010
31(I) of 2012

(b) The provisions of the Pensions Law, the Pension Benefits for Government Officers and Officers of the Wider Public Sector including Local Government Authorities (Provisions of General Application) Law as well as the provisions of any other law or Regulations made thereunder, which prescribe the rules for the payment of retirement benefits to public service officers, shall apply *mutatis mutandis* to the retirement benefits of any officer who is hired by the Authority and who previously held these rights as an officer of the public service or service

131(I) of 2012.
216(I) of 2012
52(I) of 2015
183(I) of 2015
67(I) of 2017
177(I) of 2017
16(I) of 2020.

or body of the wider public sector, having been appointed to a permanent post in the public service or in the wider public sector for the first time before 1 October 2011, as well as the benefits and pensions of dependants of such members and of the families of such members.

(c) Without prejudice to the provisions of paragraph (b), Regulations adopted pursuant to Article 45 may prescribe, regulate and provide for the establishment of:

Official Gazette Annex Three (I): 23.2.2007.
89(I) of 2001
134(I) of 2002
101(I) of 2004
62(I) of 2005
74(I) of 2017
25(I) of 2020.

(i) a health care fund to cover the members of the staff of the Authority during and after their term of service with the Authority as well as the dependants of these members, which will operate in accordance with the provisions of the Commissioner of Electronic Communications and Postal Regulation (Healthcare Fund) Regulations and the provisions of the General Healthcare System Law;

(ii) (ii) a Provident Fund to cover the employees of the Authority during their service with the Authority;

(iii)(iii) a Provident Fund for Hourly Paid Personnel to cover hourly paid members of staff of the Authority during their service with the Authority.

(5) The duties, responsibilities and qualifications of the permanent staff of the Authority shall be laid down in service plans drawn up by the Commissioner through Regulations, which shall be issued in accordance with Article 45.

(6) The organisational structure of the Authority shall be laid down in its annual budget.

47(I) of 2017.

(7) Until the Authority is adequately staffed in accordance with this Law, it shall be supported by the staff of the OCECPR, which shall be designated by the Commissioner for this purpose, in accordance with the provisions of the Secondment of Public Officers and Public Corporations Law.

Disciplinary control of the Authority's staff.

10.-(1) Matters relating to disciplinary control of the members of staff of the Authority shall be managed by the SPCA, which is established pursuant to Article 9(1).

(2) The disciplinary offences, the modus operandi of the SPCA for the purposes of disciplinary control, and the provisions and procedures under which it exercises disciplinary control over the staff of the Authority, shall be determined by Regulations adopted in accordance with Article 45.

Financing of the Authority's expenditure.
9 of 60(I) of 2025.

11.-(1)(a) The Authority shall be financed by essential and important entities, as specified in regulations adopted pursuant to Article 45.

(b) Until the Authority receives sufficient amounts of fees and revenues pursuant to this Law, for the payment of the salaries, emoluments, benefits and pensions to the members of staff of the Authority or any remuneration that is payable under service contracts concluded by the Authority in accordance with Article 14, the Republic shall pay to the Authority the amounts of salaries, emoluments, benefits, pensions, remuneration and training payable by it to its members of staff and/or service providers.

(2) All sums paid by the Republic to the Authority in accordance with paragraph 1 shall be repayable to the Republic and shall be paid by the Authority without delay:

The Republic shall not collect from the Authority any of the above amounts that it had paid to it, until the Authority has received sufficient amounts of fees and revenues under the provisions of this Law.

Representation of the Authority.

12.-(1) The Authority may sue and be sued and be a party to any civil proceedings.

(2) In any judicial proceedings or in any proceedings before any administrative or other authority, the Authority and the Commissioner, as the case may be, shall be represented by a practising lawyer and/or a member of staff of the Authority and the Commissioner shall select the lawyer or staff member.

(3) The Authority has its own seal.

(4) Any contract concluded by the Authority under this Law shall be signed by a member of staff of the Authority authorised by the Commissioner and shall bear the stamp of the Authority, certified by the signature of the

Commissioner or Deputy Commissioner.

Payments from the Authority's Fund.

13. The following payments shall be made from the Authority's Fund:

(a) To the Republic all sums repayable to it pursuant to Article 11(2);

(b) all running costs of the Authority;

(c) all amounts of salaries, emoluments, benefits and pensions payable to the members of staff of the Authority and all amounts of benefits and pensions payable in accordance with Article 9(4)(b), to the dependants and families of such members, and all amounts of remuneration payable under service contracts which are concluded by the Authority pursuant to Article 14, and all amounts of contributions payable to the funds referred to in Article 9(4)(c) as provided in regulations adopted pursuant to Article 45;

(d) all costs incurred in any appointment of an advisory body pursuant to Article 25;

(e) the amortisation of any loan concluded by the Authority pursuant to Article 7(e);

(f) any amount legally due or payable under any contract entered into by the Authority under this Law or pursuant to regulations or decisions made under this Law;

(g) any amounts legally due or payable for lawyers' fees or fees in relation to the representation of the Authority and/or the Commissioner as head of the Authority before the courts or any administrative or other authority or in relation to the provision of legal advice to the Authority;

(h) any amount which becomes legally payable as a result of the exercise of any competence, authority or duty of the Authority in accordance with the provisions of this Law or the regulations or the decisions made thereunder;

(i) to the Consolidated Fund of the Republic, all moneys collected by the Authority as an administrative fine under the provisions of this Law;

Obtaining of services by the Authority.

14. Notwithstanding the provisions of any other law, regulations, orders and decisions made under any relevant legislation, the Authority may:

173(I) of 2011.

(a) obtain services and/or equipment and/or software in matters related to the exercise of its functions and powers under this Law and the performance of its duties or for training the Authority's staff for this purpose, in accordance with the provisions of the Coordination of Procedures for the Award of Certain Works Contracts, Supply Contracts and Service Contracts by Contracting Authorities or Entities in the Fields of Defence, Security and for Related Matters Law;

(b) conclude for the above purposes service contracts in accordance with the provisions of the Coordination of Procedures for the Award of Certain Works Contracts, Supply Contracts and Service Contracts by Contracting Authorities or Entities in the Fields of Defence, Security and for Related Matters Law;

73(I) of 2016.

(c) obtain services under hire for a specific period of time from natural persons or legal entities in accordance with the provisions of the Law Regulating Public Procurement Procedures and Related Matters.

PART FOUR
GENERAL DUTIES OF THE AUTHORITY

Obligation to promote certain objectives of the Authority. 10(a) of 60(I) of 2025.

15.-(1) In the exercise of its functions and powers under the provisions of this Law and the performance of its duties, the Authority shall act in a manner that promotes the maintenance of the integrity and security of electronic communications networks and information, the achievement of a level of security of networks and information systems, including the protection of the entities under the Authority's competence.

(2) Deleted by 10(b) of 60(I) of 2025.

10(c) of 60(I) of 2025.

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

Implementation of the general policy framework by the Authority.

16.-(1) In the exercise of its functions and the performance of its powers, the Authority shall act impartially and independently, by applying the relevant general policy framework in accordance with paragraph 2.

11 of 60(I) of 2025.

(2) The Deputy Minister, shall define and/or revise the general policy framework in relation to digital security.

(3) The Deputy Minister shall publish the general policy framework in relation to digital security in the Official Gazette of the Republic.

PART FIVE
FUNCTIONS, POWERS AND DUTIES OF THE AUTHORITY

Functions, powers and duties of the Authority.

17. The Authority shall have the competence and power, inter alia, to:

(a) Deleted by 12(a) of 60(I) of 2025.

(b) implement, in matters of security of networks and information systems, the

general policy framework to be followed in accordance with Article 16(2);

12(b) of 60(I) of 2025.

(c) be a national single point of contact for the security of networks and information systems ('single point of contact');

12(c)(i)(ii) of 60(I) of 2025.

(d) exercise, as a single point of contact, liaison functions to ensure cross-border cooperation with the competent authorities of the other Member States, the competent authorities of the Republic, the cooperation group, the CSIRT network and EU-CyCLONE, as provided for in Article 33;

12(d) of 60(I) of 2025.

(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 competent authorities designated under other sector-specific EU legal acts;

12(e)(i)(ii) of 60(I) of 2025.

(f) submit as a single point of contact an annual summary report to the cooperation group, on a date to be determined by the Cooperation Group and/or the European Commission, on the notifications received, including the number of notifications and the nature of the notified incidents, as well as the measures taken in accordance with Article 35B(4) and (6);

12(f)(i)(ii) of 60(I)/2025.

(g) ensure, through the Council of Ministers, that it has sufficient resources for the effective performance of its duties and of the duties of the national CSIRT described in Article 31(3) and Article 31A(3);

(h) ensure the effective, efficient and secure cooperation of the national CSIRT within the framework of the CSIRT network referred to in Article 33;

12(g) of Law 60(I) of 2025.

(i) request the assistance of ENISA and/or other European and/or international organisations and/or other international bodies in the development of the national CSIRT;

12(h) of Law 60(I) of 2025.

(j) receive the notifications of incidents at national level and the notifications forwarded to it by any other competent authorities of Member States of the European Union in accordance with the provisions of this Law;

(k) Deleted by 12(i) of 60(I) of 2025.

12(j) of Law 60(I) of 2025.

(l) supervise the national CSIRT and other sectoral CSIRTs in the Republic:

The term 'sectoral CSIRTs' excludes the operation of a military CSIRT, which ensures effective cybersecurity cooperation with the Authority, as well as the exchange of selected information with the national CSIRT;

12(k) of 60(I) of 2025.

(m) ensure that the national CSIRTs have access to an appropriate, secure and resilient communication and information infrastructure at national level, in accordance with the provisions of this Law;

12(l) of 60(I) of 2025.
Annex I.

(n) identify for each sector and subsector referred to in Annex I or II of this Law the essential and important entities and entities providing domain name registration

Annex II. services established in the Republic;

12(m) of 60(I) of 2025. (o) review and, where necessary, update the list of identified essential and important entities and entities providing domain name registration services on a regular basis, at least every two years;

(p) cooperate closely with the Commissioner for Personal Data Protection to deal with incidents leading to personal data breaches;

12(n) of 60(I) of 2025. (q) assess the compliance of essential and important entities with their obligations under Article 35 and their impact on the security of their networks and information systems;

12(o)(i)(ii) of 60(I) of 2025. (r) ensure that essential and important entities take appropriate and proportionate technical and organisational measures to manage the risks to the security of the networks and information systems that they use in their activities;

12(p) of 60(I) of 2025. (s) ensure that essential and important entities take appropriate measures based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents;

12(q) of 60(I) of 2025. (t) ensure that essential and important entities notify the Authority, without undue delay, of any incident that has a significant impact on the provision of their services as referred to in Article 35B(3) (significant incident).

(u) Deleted by 12(r) of 60(I) of 2025.

(v) Deleted by 12(r) of 60(I) of 2025.

(w) Deleted by 12(r) of 60(I) of 2025.

(x) Deleted by 12(r) of 60(I) of 2025.

(y) issue any decision, including interim measures, in respect of matters falling within its functions;

12(s) of 60(I) of 2025. (z) impose an administrative fine, in accordance with Articles 43 and 43A, on any person that violates the provisions of this Law or the provisions of the regulations or decisions made thereunder;

(aa) be a member of and participate in meetings of such European or international organisations in the interest of the Republic;

12(t) of 60(I) of 2025. (bb) request, in the context of its specific activities, the provision by essential and/or important 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, subject to the principle of proportionality;

(cc) exercise any other functions, powers and duties provided to it under the provisions of this Law or under the provisions of the regulations and decisions made thereunder;

125(I) of 2018. (dd) process personal data, pursuant to the provisions of this Law, 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)

No 2016/679;

12(u) of 60(I) of 2025.

(ee) adopt and/or maintain provisions aimed at achieving a higher level of security of networks and information systems, without prejudice to the provisions the obligations of the Republic deriving from Union law;

(ff) subject to the provisions of Article 19(3), publish information and documents referred to in Article 19 as it deems appropriate, for the purposes of promoting public awareness and understanding on issues of security of networks and information systems, digital security and cybersecurity;

(gg) monitor the application of the provisions of this Law in the Republic and, in the exercise of its competence, it may request and receive assistance from persons subject to supervision, under any relevant legislation, and from the respective supervisory authorities or from the national authorities contributing to supervision, when it is carried out by supranational authorities:

The powers granted to the Authority under the provisions of this Law shall be exercised in such a way so as not to prejudice the functions, duties and powers of the supervisory, national or transnational authorities referred to in the provisions of this paragraph;

12(v) of 60(I) of 2025.

(hh) conclude memoranda of understanding with bodies governed by this Law or other authorities or organizations or companies that cooperate with the Authority:

12(v) of 60(I) of 2025.

The Authority may conclude memoranda of cooperation with third countries' national computer security incident response teams and, in this context, the Authority shall facilitate the effective, efficient and secure exchange of information with those national computer security incident response teams of a third country, using relevant information exchange protocols, including the **Traffic Light Protocol (TLP)**:

12(v) of 60(I) of 2025.

The Authority may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with the provisions of 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;

12(w)(i)(ii) of 60(I) of 2025.

(ii) conclude, subject to the provisions of any other legal acts issued by the European Union, memoranda of cooperation and/or agreements, where deemed necessary, with supervisory authorities, supervising licensed institutions to which the provisions of this Law apply, and such memoranda of cooperation and/or agreements may specify how the provisions triggered by the designation of authorised institutions as essential or important entities are to be applied or otherwise;

12(x) of 60(I) of 2025.

(jj) issue, in the context of the effective exercise of its competences and powers, decisions on the implementation of Union regulations, on the harmonisation with EU directives, decisions, implementing regulations, delegated regulations, recommendations and any other relevant European Union acts and/or on the clarification of the provisions of this Law;

12(x) of 60(I) of 2025.

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

12(x) of 60(I) of 2025.

(ll) receive notifications of serious incidents pursuant to Article 35b, as well as incidents of cyberthreats and near misses pursuant to Article 42;

12(x) of 60(I) of 2025.

(mm) participate in peer reviews pursuant to Article 34A;

12(x) of 60(I) of 2025.

(nn) use the necessary means to exercise effective supervision of the entities falling within the scope of this Law and take the necessary measures to ensure their compliance under the provisions of this Law, and

12(x) of 60(I) of 2025.

(oo) establish and maintain a register of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content distribution network providers, managed service providers, security service providers as well as providers of online marketplaces, providers of online search engines or providers of social networking services, subject to the provisions of Article 37A.

General obligation.

18. The Authority must ensure that the principles of equal treatment, objectivity and proportionality are respected in the exercise of those powers.

PART SIX
OBTAINING INFORMATION AND OTHER POWERS, ORDERS, DECISIONS, INVESTIGATIONS AND ADVISORY BODIES

Obtaining information.

19.-(1) In order to ensure the better carrying out of its functions and powers, the Authority, in compliance with the principle of proportionality, shall, by means of a reasoned request, have the power to require from:

13(a) of 60(I) of 2025.

(a) Deleted by 13(a) of 60(I) of 2025.

13(a) of 60(I) of 2025.

(a1) essential and/or important entities and/or providers of fixed and mobile communications, such as, subject to the provisions of Article 2(2) and (3) and where the Authority deems appropriate at the request of the police and/or the Cypriot Information Service, to provide the Authority and/or the police and/or the Cypriot Information Service with the necessary information for public order and national security purposes;

13(b)(i)(ii)(iii)(iv)(v) of 60(I) of 2025.

(b) essential and/or important entities to provide the necessary information for the assessment of the security of networks and information systems, including, but not limited to, documented security policies and/or evidence demonstrating the effective implementation of security policies, such as results of a security inspection that is carried out either by the Authority itself or by an authorised inspector and in the latter case, to make available the results as well as the relevant data at its disposal and the requested information shall be used and maintained by the Authority in order to ensure the compliance of the essential and/or important entities with their obligations arising from the provisions of this Law, the provisions of the regulations made under this Law and the provisions of the Decisions of the Authority issued for the application of this Law;

13(b) of 60(I)/2025.

Information obtained by the Authority in accordance with this paragraph shall concern the promotion of the objects referred to in Articles 15 and 16 and the performance of the functions, powers and duties of the Authority which are set out in the provisions of Article 17 and may not be used for any purpose other than the purpose for which it was requested.

(c) Deleted by 13(c) of 60(I) of 2025.

Reservation deleted by 13(d) of 60(I) of 2025.

13(e)(i)(ii) of 60(I) of 2025.

(2)(a) Persons who are required to submit information in accordance with this Article shall respond in within a specified time limit, in accordance with Article 18 and Article 19(1), and provide the details and information requested by the Authority.

13(f) of 60(I) of 2025.

(b) each essential and/or important entity shall provide the Authority with any information, as specified in paragraph (1), upon a reasoned request from the Authority and in accordance with the timeframe and scope of detail set out in the relevant request.

(c) Where a person fails to comply with the Authority's request for information in accordance with this Article, an administrative fine of up to five thousand euro (EUR 5 000) shall be imposed.

(d) The Authority shall, upon a reasoned request from the Commission, provide it with the necessary information relating to the performance of its duties and the information required shall be proportionate to the purpose of carrying out those duties.

13(g) of Law 60(I) of 2025.

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

13(h) of Law 60(I) of 2025.

(3)(a) The Authority shall preserve and accept as confidential any information provided by a person which is classified by such person as confidential, except where the Authority decides otherwise for the purposes of exercising its powers and must document its decision on disclosure of the information.

13(i) of 60(I) of 2025.

(b) The Authority shall not disclose information that is covered by an obligation of professional secrecy and in particular information concerning essential and/or important entities, their business relationships or their invoicing and this prohibition is without prejudice to the right of the Authority to disclose information where this is fundamental for the purpose of fulfilling its duties:

In such a case, any disclosure shall be proportionate and shall take into account the legitimate interests of individuals in safeguarding their business secrets.

Other powers.

20.-(1) The Authority shall have the power to:

14(a)(i) of 60(I) of 2025.

(a) supervise compliance with the obligations imposed by this Law and/or the decisions adopted under the provisions of this Law, on essential and/or important entities;

14(a)(ii)(aa)(bb) of 60(I) of 2025.

(b) require from any essential and/or important entity or any other person, any information that it may reasonably consider necessary for the purpose of exercising its functions and powers and performing its duties, including information stemming from the installation of sensors, for the purpose of detecting malware on internal networks and/or on external networks without prejudice to Article 31A (4)

and (5):

14(a)(iii) of 60(I) of 2025.

The installation of sensors by the Authority in internal networks can only be done at the request or consent of the essential and/or important entity and/or for national security reasons, in compliance with Article 15(3);

14(a)(iv) of 60(I) of 2025.

(c) determine, by decision, cybersecurity risk-management measures and procedures for the notification of digital security breaches and supervise compliance with them and, where necessary, order corrective measures;

(d) issue any decisions which are necessary to ensure compliance with the provisions of this Law;

14(a)(v) of 60(I) of 2025.

(e) impose administrative fines on essential and/or important entities for the violation of the provisions of this Law or of the decisions adopted thereunder;

(f) summon and compel, in the manner laid down in a decision, the presence of witnesses in investigations.

14(b) of 60(I) of 2025.

(2) The Commissioner shall authorise any employee of the Authority to enter, inspect, investigate, carry out an audit, at any reasonable time, in any area, premises or vehicle, excluding any area that is used as a residence, which are used for the provision of any services by essential and important entities, in accordance with the provisions of this Law, and shall collect data that may be used for purposes of proof or in any judicial proceedings regarding any violation or failure to comply with the provisions of this Law or the provisions of the regulations or decisions made thereunder.

(3) Any person who, personally or through an employee or other representative, obstructs or prevents an Authority employee from performing any of their duties in accordance with paragraph (2), shall be guilty of an offence and shall, if convicted, be liable to imprisonment for a term not exceeding six (6) months or to a fine not exceeding eight thousand euro (EUR 8 000) or to both such penalties.

Adoption of decisions.

21.-(1) Prior to the adoption of a decision pursuant to Article 20(1)(d), any person who, in the Authority's opinion, is affected or may be affected by the decision, shall be notified and given the opportunity to be heard within ten (10) working days of notification of the decision.

The Authority shall not be obliged to give notice prior to the issuance of a decision in urgent cases at the absolute discretion of the Authority, but in such cases the Authority shall offer the affected person the opportunity to be heard, within ten (10) working days from the issuance of the decision, as to why the decision should be revoked or amended.

(2) After the affected person is heard, in accordance with paragraph (1), the Commissioner shall issue and notify his final decision to anyone concerned as soon as possible.

Criminal offence.

22. Any person who, without reasonable cause, fails to comply with Article 21 is committing a criminal offence and, if convicted, shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding five thousand euro (EUR 5 000) or to both such penalties.

Carrying out of an investigation.

23.-(1) The Authority may, on its own initiative, carry out an investigation into activities and operations of any essential and/or important entity which are deemed

15 of 60(I) of 2025.

to be inconsistent with the provisions and with the application of this Law, and consequently make recommendations and issue decisions as it considers appropriate.

(2) For the purposes of carrying out an investigation in accordance with paragraph (1), the Authority may:

(a) summon witnesses and interested parties in the manner specified in a decision or regulations, produce, present and submit documents, books, plans and records;

(b) examine witnesses and interested parties.

(3) Any person shall commit a criminal offence when:

(a) without reasonable cause omits or refuses to comply with a summons to appear before the Authority or to produce, present or submit documents, books, plans or records; or

(b) while being a witness, refuses to answer any reasonable question put to him without reasonable cause:

In any case, no one is obliged to answer, if the answer may incriminate him in relation to a criminal offence or if it constitutes a breach of secrecy of communication between a lawyer and a client and/or hinders or interrupts the proceedings before the Authority.

(4) Any person who is convicted of a criminal offence in contravention of paragraph (3)(a) and/or (b) shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding five thousand euro (EUR 5 000) or to both such penalties.

(5) Any person may be represented before the Authority by a lawyer and may summon any witnesses in the manner specified in the decision.

(6) The Commissioner or an officer of the Authority who is authorised by the Commissioner shall carry out any proceedings before the Authority and shall have the power to restrict or suppress the abuse of the proceedings before it.

Consultations/ Hearings.
16 of 60(I) of 2025.

24.-(a) The Authority may carry out consultations with representatives of the Republic, with essential and/or important entities and with any other persons or organisations, as the Authority deems appropriate from time to time.

(b) The procedure for carrying out consultations may be regulated by a relevant decision of the Authority.

(c) The Authority may, where appropriate, in relation to the application of its functions and powers, hold public hearings, and the procedure for carrying out public hearings may be regulated by a relevant decision of the Authority.

(d) The Authority may adopt a decision laying down the procedure for the hearing of persons, in particular in cases of imposition of administrative fines and/or other administrative penalties.

Appointment of advisory bodies.

25. The Authority may establish advisory bodies to advise it on such matters as it may deem appropriate from time to time, appoint their members and pay the relevant costs from the Authority's Fund.

Adoption of interim measures. 17 of 60(I) of 2025.

26.-(a) The Authority may, by virtue of its powers and in particular upon request by an interested essential and/or important entity or organisation, take interim measures, including the adoption of an interim decision, in particular in cases where there is a potential risk to the security of networks and information systems.

(b) In such cases, the Authority shall request the affected parties to express their views, within ten (10) working days from the issuance of a decision, as to whether the decision should be revoked or amended.

(c) After a hearing, the Authority shall adopt and notify its final decision as soon as possible.

18 of 60(I) of 2025.

PART SEVEN

IDENTIFICATION OF ESSENTIAL AND IMPORTANT ENTITIES

19 of 60(I) of 2025. Essential and important entities.

27.- (1)(a) For the purposes of this Law, the following entities shall be considered to be essential entities:

Annex I.

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

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

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

(iv) public administration entities referred to in Article 2A(2)(f)(i);

Annex I. Annex II.

(v) any other entities of the types referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2A(2)(b) to (e);

(vi) entities identified as critical entities by the competent authority for the resilience of critical entities, referred to in Article 2A(3); and

(vii) entities which the Authority identified before 16 January 2023 as operators of essential services or operators of critical information infrastructure, in accordance with the Commissioner's decisions of 17 August 2020 and 8 November 2021, which were issued or replaced pursuant to the provisions of the Security of Networks and Information Systems Law of 2020.

The Commissioner's decisions dated 17 August 2020 and 8 November 2021 shall continue to be in force until they are replaced, following a criticality assessment, as provided for in Article 27(1)(b); and

(b) For the purposes of applying the provisions of paragraph (1)(a), and unless otherwise provided for in this Law, the Authority may designate entities as essential entities following a criticality assessment, based on criteria defined by the Authority after consulting the Deputy Minister, in compliance with paragraph (7) of this Article:

The criteria for the criticality assessment work shall be laid down by the Authority and approved by a decision of the Council of Ministers before they apply, and shall

apply 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 do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities. This includes entities identified by the Authority as important entities pursuant to Article 2A(2)(b) to (e).

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

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

(a) the name of the entity;

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

Annex I.
Annex II.

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

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

The entities referred to in the paragraph 3 shall notify any changes to the details submitted pursuant to this paragraph without delay, and, in any event, within two (2) weeks of the date of the change:

The Authority may establish national mechanisms for entities to register themselves:

The Authority shall take into account guidelines and templates adopted by the Commission regarding the obligations set out in paragraph 3.

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

Annex I.
Annex II.

(a) the Commission and the Cooperation Group of the number of essential and important entities listed pursuant to paragraph 3 for each sector and sub-sector referred to in Annex I or II; and

Annex I.
Annex II.

(b) the Commission of relevant information about the number of essential and important entities identified pursuant to Article 2(2)(b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Article 2A(2)(b) to (e), pursuant to which they were identified.

(6) The Authority may, at the request of the Commission, notify the Commission of the names of essential and important entities referred to in paragraph (5)(b).

(7) The results of the assessment carried out by the Authority and the list of essential and important entities, entities providing domain name registration services and entities exempted pursuant to Article 2(4) of this Law, drawn up by

the Authority pursuant to this Article, shall be adopted by a decision of the Council of Ministers, which shall be designated as confidential and shall not be published in the Government Gazette of the Republic of Cyprus:
The results of the assessment and the list of essential and important entities and entities providing domain name registration services approved by the decision of the Council of Ministers shall be confidential and shall not be published in the Government Gazette of the Republic of Cyprus.

(8) Essential and important entities approved by a decision of the Council of Ministers pursuant to paragraph 7 shall be designated by a decision issued by the Authority, which shall be served on the essential or important entity in question.

20 of 60(I) of 2025. Security by design.

27A. Newly created entities in the Republic, which fall under the scope of this Law and which may be identified as essential or important entities, pursuant to Article 27, shall inform and seek the opinion and/or guidance of the Authority on the security measures to be taken from the design/creation (security by design) of their computer infrastructure and the obligations to which they are subject from the date of commencement of the provision of their services, in accordance with Article 39.

20 of 60(I) of 2025. Obligation to inform the Authority.

27B. Without prejudice to Article 27, newly created entities and/or entities falling within the scope of Article 2A of this Law that were not included in the list of essential and important entities established by the Authority in accordance with Article 27(3) must inform the Authority for the purpose of their assessment.

Significant disruption.

28. Deleted by 21 of 60 (I) of 2025.

PART EIGHT
FRAMEWORK ON THE SECURITY OF NETWORKS AND INFORMATION SYSTEMS

22 of 60(I) of 2025. National cybersecurity strategy.

29.-(1)(a) The Deputy Minister shall establish a general policy framework in relation to digital security pursuant to Article 16 and shall forward to the Council of Ministers for approval the cybersecurity strategy. The preparation of that strategy shall seriously take into account relevant recommendations and/or guidelines from the Authority.

(b) The cybersecurity strategy plan shall provide for the strategic objectives, the resources required to achieve those objectives, appropriate policy 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 sectors referred to in Annexes I and II;

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

(iii) a governance framework clarifying the roles and responsibilities of the 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 those bodies and the competent authorities on the basis of sector-specific Union legal acts;

(iv) a mechanism for the identification of relevant assets and risk assessment at national level;

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

(vi) a list of the different 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 on the resilience of critical entities, for the purpose of exchanging information on risks, cyberthreats and incidents and on risks, threats and incidents outside the cyberspace and exercising supervisory tasks, where appropriate; and

(viii) a plan, including the necessary measures, to increase 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) the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;

(c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 31B(1);

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

(e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;

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

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

(h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;

(i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope

of this Law, by providing easily accessible guidance and assistance for their specific needs; and

(j) promoting active cyber protection.

Active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the network of entities:

The Authority's services, taking into account, inter alia, the availability of the Authority's resources and/or 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 the installation of sensors, in accordance with Article 20(1)(b).

(3)(a) The Authority shall assess the national cybersecurity strategy on a regular basis and at least every four (4) years on the basis of key performance indicators and recommend that it be updated.

b) ENISA shall assist the Authority, upon its request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Law.

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

(b) The Authority may exclude information which relates to national security from such notifications.

23(a)(b) of Law 60(I) of 2025. Competent national authority and single point of contact. 17(I) of 2018.

30.- (1) the Authority designated as the competent national authority for the security of networks and information systems, in accordance with the provisions of the Security of Networks and Information Systems Law of 2018, shall continue to be the competent authority for cybersecurity, shall have the supervisory and enforcement duties provided for in the provisions of this Law and shall have the functions of the cyber crisis management authority pursuant to Article 32A.

23(Y)(i)(ii)(iii) of 60(I) of 2025.

(2) The Authority designated as the competent national authority to coordinate the implementation of the cybersecurity strategy, in accordance with the Security of Networks and Information Systems Law of 2018, and as the authority responsible for coordinating the implementation of the cybersecurity strategy, shall continue to be the competent national authority for coordinating the implementation of the national cybersecurity strategy.

(3) The Authority shall monitor the application of the provisions of this Law in the Republic.

23(d) of 60(I) of 2025.

(4) the Authority shall be designated as the national single point of contact for cybersecurity.

23(e)(i)(ii) of 60(I) of 2025.

(5) the Authority, as a single point of contact, shall exercise a liaison function to ensure the cross-border cooperation of the Republic with the competent authorities of other Member States, and where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities

within the Republic.

23(f) of 60(I) of 2025.

(6) the Authority shall ensure that it has the necessary powers and sufficient resources to perform effectively and efficiently the tasks assigned to it and thereby achieve the objectives of the provisions of this Law and shall ensure the effective, efficient and safe cooperation of its representatives appointed within the Cooperation Group.

23(g) of Law 60(I) of 2025.

Official Journal of the EU: L 212, 22.8.2018, p. 1.

(7) In order to ensure the effective performance of the Authority's tasks and obligations, as a competent authority and as a single point of contact, the Authority shall to the extent possible ensure appropriate cooperation between the competent national law enforcement authorities, the Cyprus Information 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, (yy) 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 pursuant to Regulation (EU) 2022/2554, the OCECPR, the Central Bank of Cyprus as the national macro-prudential authority and the competent authority of the Republic for the resilience of critical entities, and the competent authorities under other sector-specific EU legal acts, within the Republic.

24 of 60(I) of 2025. Computer security incident response team (national CSIRT). Annex I. Annex II.

31.-(1) The national CSIRT shall comply with the requirements set out in Article 31A(1), shall cover at least the sectors, subsectors and types of entities referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.

(2) The national CSIRT shall have at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders and contribute to the deployment of secure information sharing and cybersecurity tools.

(3) The Authority shall ensure that the national CSIRT has sufficient resources to effectively carry out its tasks, in accordance with Article 31A(4).

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

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

(6) The Authority shall ensure the effective, efficient and secure cooperation of the national CSIRTs within the CSIRT network.

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

(8) The national CSIRT may cooperate with third countries' national computer security incident response teams (CSIRTs) or equivalent third-country bodies, and

where necessary through the Cyprus Intelligence Service, in particular for the purpose of providing cybersecurity assistance and/or implementing Article 17(hh):

This cooperation and the exchange of the relevant information with third countries' national computer security incident response teams (CSIRTs) including personal data, shall be carried out 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.

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

(10)(a) Regulation (EU) 2022/2554 shall be considered to be a sector-specific Union legal act in relation to this Law with regard to financial sector entities.

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

(c) The provisions of this Law on cybersecurity risk-management and reporting obligations, and supervision and enforcement shall not apply to financial entities covered by Regulation (EU) 2022/2554.

(11) Pursuant to Regulation (EU) 2022/2554, the competent authorities of the Republic are expected to cooperate with the national CSIRT on large-scale incidents or cyberthreats with a significant impact in order to facilitate cross-sectoral learning and contribute to the prevention and management of cyberattacks.

(12) With a view to maintaining a strong relationship and the exchange of information with the financial sector, the European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group, exchange information and cooperate with the Authority.

25 of 60(I) of 2025. Requirements, technical capabilities and tasks of the national CSIRT.

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

(a) it shall ensure a high level of availability of its communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times; it shall clearly specify the communication channels and make them known to supervised entities and cooperative partners;

(b) the national CSIRT's premises and the supporting information systems shall be located at secure sites;

(c) it shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;

(d) it shall ensure the confidentiality and trustworthiness of its operations;

(e) it shall be adequately staffed to ensure availability of its services at all

times and it shall ensure that its staff is trained appropriately;

(f) it shall be equipped with redundant systems and backup working space to ensure 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 necessary to carry out the tasks referred to paragraph 4.

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

(4) The national CSIRT shall have the following tasks:

(a) monitoring and analysing cyberthreats, vulnerabilities and incidents at national level and, upon request and/or pursuant to Article 15(3), providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information to the essential and important entities concerned and to the competent authorities, other relevant stakeholders and interested parties, and other interested parties at the Authority's discretion, on cyberthreats, vulnerabilities and incidents, if possible in near real-time;

(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(e) providing, upon the request of an essential or important entity, a proactive scanning and/or penetration testing of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

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

(g) acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 31B(1) and (2);

(h) contributing to the deployment of secure information-sharing tools pursuant to Article 31(2):

When carrying out the tasks referred to in this paragraph, the national CSIRT may prioritise particular tasks on the basis of a risk-based approach.

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

(b) Such scanning shall be carried out to detect vulnerable or insecurely configured

network and information systems and inform the entities concerned.

(c) Such scanning shall not have any negative impact on the functioning of the entities' services.

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

(a) incident-handling procedures;

(b) crisis management; and

(c) coordinated vulnerability disclosure under Article 31B(1) and (2).

25 of 60(I) of 2025. Coordinated vulnerability disclosure and a European vulnerability database.

31B.-(1) For the purposes of coordinated vulnerability disclosure, the national CSIRT shall be designated as coordinator and, in accordance with its coordinating tasks, shall act as a trusted intermediary, facilitating, where necessary, interaction between the natural person or legal entity reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party.

(2) The tasks of the CSIRT appointed as coordinator shall include:

(a) identifying and contacting the entities concerned;

(b) assisting the natural persons or legal entities reporting a vulnerability; and

(c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

(3)(a) The Authority shall ensure that natural persons or legal entities are able to report, anonymously where they so request, a vulnerability to the national CSIRT.

(b) The national CSIRT shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural person or legal entity reporting the vulnerability.

(c) Where a reported vulnerability could have a significant impact on entities in more than one Member State, the national CSIRT shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRT network.

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

Cooperation at national level.

32.-(1) the Authority, as the competent authority, the single point of contact and the national CSIRT, shall cooperate with the sectoral CSIRTs and other competent authorities with regard to the fulfilment of the obligations laid down in this Law.

(2) The Authority shall receive notifications of significant incidents pursuant to Article 35B, and incidents, cyberthreats and near misses pursuant to Article 42.

(3) In order to carry out its tasks, the Authority, as a single point of contact, shall be kept informed of notifications of incidents, cyberthreats and near misses

submitted pursuant to the provisions of this Law and in compliance with Article 17(l), Article 30(7) and Article 31(10).

(4) (a) The Authority and the competent authority for the resilience of critical entities cooperate and exchange information regularly on the identification of critical entities, on risks, cyberthreats, and incidents and non-cyber risks, threats and incidents affecting entities identified as critical entities by the competent authority for the resilience of critical entities and the measures taken in response to such risks, threats and incidents.

(b) The competent authorities of the Republic pursuant to Regulation (EU) 2022/2554, the OCECPR and the Department of Electronic Communications, the Central Bank of Cyprus as the national macroprudential authority and other competent authorities shall exchange relevant information on a regular basis, including with regard to relevant incidents and cyberthreats.

(5) The Authority shall simplify the reporting through technical means for notifications referred to in Articles 35B and 42 of this Law.

27 of 60(I) of 2025. National cyber crisis management framework.

32A.-(1) As the authority responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authority), the Authority shall ensure that it has adequate resources to carry out, in an effective and efficient manner, the tasks assigned to it and shall also ensure coherence with the existing frameworks for general national cybersecurity crisis management.

(2) The Authority shall act as a coordinator for the management of large-scale cybersecurity incidents and crises in cooperation with the competent authorities of the Republic under relevant laws of the Republic or sector-specific Union legal acts:

Where the financial sector is involved, the Authority shall serve as the coordinator in cooperation with the Central Bank of Cyprus as the national macroprudential authority.

(3) The Authority shall identify capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Law.

(4) The Authority shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out.

(5) The national large-scale cybersecurity incident and crisis response plan shall be adopted by a decision of the Council of Ministers, which shall be classified as confidential and shall not be published in the Government Gazette of the Republic.

(6) That plan shall lay down, in particular:

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

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

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

(d) national preparedness measures, including exercises and training

activities;

(e) the relevant public and private stakeholders and infrastructure involved; and

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

(7) The Authority shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 of this Article about the national large-scale cybersecurity incident and crisis response plan within three months of the adoption of that plan.

(8) Upon the approval of the Council of Ministers, the Authority may exclude information where and to the extent that such exclusion is necessary for national security purposes.

(9) The Authority may request that the European cyber crisis liaison organisation network (EU-CyCLONe) discusses the national large-scale cybersecurity incident and crisis response plan, in accordance with Article 16(3)(e) of Directive (EU) 2022/2555.

28 of 60(I) of 2025.

PART NINE

COOPERATION AND PEER REVIEWS

29(a)(b) of 60(I) of 2025. Cooperation Group, CSIRT network and European cyber crisis liaison organisation network (EU-CyCLONe).

33.- (1) Representatives of the Authority, pursuant to Article 8(2) of Directive (EU) 2022/2555, shall participate in the Cooperation Group established and operating pursuant to Article 14 of Directive (EU) 2022/2555 and shall contribute to the relevant work of the Cooperation Group, including, inter alia, as laid down in Articles 14 and 22 of Directive (EU) 2022/2555.

29(c)(i)(ii) of 60(I)/2025.

(2) Representatives of the Authority and/or the national CSIRT shall participate in the CSIRT network established and operated in accordance with Article 15 of Directive (EU) 2022/2555 and contribute to the performance of its tasks.

(3) Representatives of the Authority and/or the national CSIRT shall cooperate with bodies at European level and represent the Republic on matters related to its competences.

29(d) of 60(I) of 2025.

(4) Subject to the provisions of Article 32A, representatives of the Authority shall participate in the EU-CyCLONe, which has been established on the basis of the provisions of Article 16 of Directive (EU) 2022/2555, and shall actively contribute to its relevant work.

Cooperation with national and international bodies.

34. The Authority may:

(a) cooperate with private and public sector bodies at national level;

(b) cooperate with private and public sector bodies at international level and represent the Republic in international organisations in matters falling within its competence, without prejudice to what is otherwise laid down in international agreements.

30 of 60(I) of 2025.

(c) participate effectively in exchange programmes for officials from other Member States, within a specific framework and, where appropriate, by obtaining the required security clearance for officials participating in such exchange programmes, with a view to improving cooperation and enhancing the trust of the Member States.

31 of 60(I) of 2025.
Peer reviews.

34A.- (1)(a) The Authority shall participate in peer reviews on a voluntary basis.

(b) Peer reviews shall be carried out pursuant to Article 19 of Directive (EU) 2022/2555 by cybersecurity experts.

(c) The cybersecurity experts shall be designated by at least two (2) Member States, different from the Member State being reviewed.

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

(a) the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down 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 exercise of the tasks of the competent authorities;

(c) the operational capabilities of the CSIRTs;

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

(e) the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29 of Directive (EU) 2022/2555; and

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

(3)(a) The Authority shall designate cybersecurity experts eligible to carry out the peer reviews based on objective, non-discriminatory, fair and transparent criteria, in accordance with the methodology developed by the Cooperation Group, as provided for in Article 19(1) of Directive (EU) 2022/2555.

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

(4) The Authority may identify specific issues as referred to in paragraph 2, point (f), for the purposes of a peer review.

(5) Before commencing a peer review as referred to in paragraph 1, the Authority shall notify the participating Member States of the scope of the peer review, including the specific issues identified pursuant to paragraph 4.

(6)(a) Prior to the commencement of the peer review, the Authority may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts.

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

(7)(a) Peer reviews shall entail physical or virtual on-site visits and off-site

exchanges of information.

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

(c) Any information obtained through the peer review shall be used solely for that purpose.

(d) The cybersecurity experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties:

The cybersecurity experts designated by the Authority shall take into account the codes of conduct issued by the Cooperation Group in cooperation with the Commission and ENISA.

(8) The peer reviewed aspects shall not be subject to a further peer review for two (2) years following the conclusion of the peer review, unless otherwise requested by the party reviewed or agreed upon after a proposal of the Cooperation Group.

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

(b) The Authority subject to the peer review may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State.

(10)(a) Cybersecurity experts participating in peer reviews shall draft reports on the findings and conclusions of the peer reviews which shall include recommendations to enable improvement on the aspects covered by the peer review.

(b) The Authority may provide comments on the draft reports concerning it and such comments shall be attached to the reports.

(c) The reports shall be submitted to the Cooperation Group and the CSIRTs network where relevant.

(d) The Authority may make its report, or a redacted version of it, publicly available.

31 of 60(I) of 2025. Cybersecurity information-sharing arrangements.

34B.- (1) Essential and important entities falling within the scope of this Law and, where relevant, other entities not falling within the scope of this Law are able to exchange relevant cybersecurity information among themselves on a voluntary basis, including information relating to cyberthreats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

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

(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyberthreats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyberthreat research between public and private entities.

(2)(a) The exchange of information shall take place within communities of essential and important entities, and where relevant, their suppliers or service providers.

(b) The exchange of information shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

(3)(a) The Authority shall establish cybersecurity information-sharing arrangements referred to in the provisions of paragraph 2.

(b) Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements.

(c) In laying down the details of the involvement of public authorities

in such arrangements, the Authority may impose conditions on the information made available by it.

(d) The Authority shall offer assistance for the application of such arrangements in accordance with the policies referred to in Article 29(2), point (h).

(4) Essential and important entities shall notify the Authority of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of its withdrawal from such arrangements, once the withdrawal takes effect.

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

31 of 60(I) of 2025. Mutual assistance.

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 and the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary.

(b) That cooperation shall entail, at least, that:

(i) Where the Authority applies supervisory or enforcement measures in the Republic, it shall inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken and vice versa;

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

(iii) The Authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures

can be implemented in an effective, efficient and consistent manner and vice versa:

The mutual assistance referred to point (iii), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits:

When receiving a request for assistance, the Authority shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to its supervisory tasks, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Republic's national security, public security or defence.

Before refusing such a request, the Authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA.

(2) Where appropriate and with common agreement, the Authority may carry out joint supervisory actions with other competent authorities of various Member States.

32 of 60(I) of 2025.

PART TEN

CYBERSECURITY RISK-MANAGEMENT MEASURES, REPORTING OBLIGATIONS, SUPERVISION AND ENFORCEMENT

33 of 60(I) of 2025. Cybersecurity risk-management measures.

35.- (1)(a) Essential and important entities shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

(b) Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in paragraph 1(a) shall ensure a level of security of network and information systems appropriate to the risks posed.

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

(2) The measures referred to in paragraph 1(a), which may be laid down in a decision adopted by the Authority, shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system 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) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

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

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

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

(a) the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures; and

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

(4) An entity that finds that it does not comply with the measures provided for in paragraph 2 must takes without undue delay, all necessary, appropriate and proportionate corrective measures.

(5) The Authority shall apply any implementing acts of the Commission laying down the technical and the methodological requirements of the measures referred to in paragraph 2, in accordance with Article 21(5) of Directive (EU) 2022/2555.

34 of 60(I) of 2025. Governance.

35A.-(1) The management bodies of essential and important entities must approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 35, oversee their implementation and may be held liable for infringements by the entities of that Article.

(2) The application of the provisions of paragraph 1 shall be without prejudice to the applicable law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

(3) The members of the management bodies of essential and important entities are required to follow training, and shall offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

34 of 60(I) of 2025. Reporting obligations.

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

(b) Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect

the provision of those services.
(c) Those entities report, inter alia, any information enabling the Authority to determine any cross-border impact of the incident.

(d) The mere act of notification shall not subject the notifying entity to increased liability.

(e) Where the entities concerned notify the competent authority of a significant incident under paragraph 1, points (a) to (d), the Authority shall forward the notification to the national CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, the Authority, as a single point of contact, shall ensure that it is provided in due time with relevant information notified in accordance with paragraph 4 and, where the Authority considers it necessary, in consultation with other competent authorities.

(g) The procedures and content of incident notification and any related information shall be regulated by a decision issued by the Authority pursuant to the provisions of this Law.

(2) Where applicable, essential and important entities shall, without undue delay, notify recipients of their services that are potentially affected by a significant cyberthreat any measures or remedies that those recipients are able to take in response to that threat and, where appropriate, the entities shall also inform those recipients of the significant cyberthreat itself:

Without prejudice to paragraph 7, where there are serious reasons for not informing the recipients, the entity must notify, consult and obtain approval from the Authority.

(3) An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; and/or

(b) it has affected or is capable of affecting other natural persons or legal entities by causing considerable material or non-material damage.

(4) For the purpose of notification under paragraph 1, the essential 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, a warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within seventy-two (72) hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of the Authority, an intermediate report on relevant status updates;

(d) a final report not later than one month after the submission of the incident

notification under point (b) or (f), including the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied 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 the submission of the final report referred to in point (d), essential and important entities provide a progress report every fifteen (15) days, after the submission of the incident notification in accordance with point (b) or (f), until the submission of the final report within fifteen (15) days of the restoration of the functioning of the affected network or information system; and

(f) By way of derogation from point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the Authority, without undue delay and in any event within twenty-four (24) hours of becoming aware of the significant incident.

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

(b) The national CSIRT shall provide additional technical support if the entity concerned so requests or if the Authority considers it necessary.

(c) Where the significant incident is suspected to be of criminal nature, the Authority shall also provide guidance on reporting 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 inform, without undue delay, the other affected Member States and ENISA of the significant incident.

(b) Such information shall include the type of information received in accordance with paragraph 4.

(c) In so doing, the Authority shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

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

(8) As a single point of contact, the Authority shall, where appropriate, forward notifications received pursuant to paragraph 1 to the single points of contact of

other affected Member States.

(9)(a) The Authority shall submit a summary report to ENISA every three (3) months, including anonymised and aggregated data on significant incidents, incidents, cyberthreats and near misses notified in accordance with paragraph 1 of this Article and with Article 42 of this Law.

(b) The Authority shall take into account any technical guidance adopted 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 information about significant incidents, incidents, cyberthreats and near misses notified in accordance with paragraph 1 of this Article and with Article 42 by entities identified as critical entities by the competent authority for the resilience of critical entities.

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

(12)(a) Where provisions of a sector-specific Union legal act require essential or important entities to comply with reporting obligations that are at least equivalent in effect to the reporting obligations laid down in this Law, the consistency and effectiveness of the handling of incident notifications should be ensured.

(b) To that end, the provisions relating to incident notifications of the sector-specific Union legal act should provide the Authority with an immediate access to the incident notifications submitted in accordance with the sector-specific Union legal act. In particular, such immediate access can be ensured if incident notifications are being forwarded without undue delay to the Authority.

(c) Where appropriate, the Authority should put in place an automatic and direct reporting mechanism that ensures systematic and immediate sharing of information concerning the handling of such incident notifications.

(d) For the purpose of simplifying reporting and of implementing the automatic and direct reporting mechanism, the Authority could, in accordance with the sector-specific Union legal act, use a single entry point.

35(a)(b) of 60(I) of 2025. Supervision and enforcement.

36.- (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 in accordance with this Law.

35(b) of 60(I) of 2025.

(2) The Authority may adopt a decision on how to assess the compliance of essential and important entities falling within the scope of this Law with regard to their obligations.

35(b) of 60(I) of 2025.

(3)(a) The Authority may prioritise supervisory tasks and such prioritisation shall be based on a risk-based approach.

(b) To that end, when exercising their supervisory tasks provided for in Articles 36A and 36B, the Authority may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

(4) Deleted by 35(c) of 60(I) of 2025.

(5) Deleted by 35(c) of 60(I) of 2025.

(6) Deleted by 35(c) of 60(I) of 2025.

35(d) of 60(I) of 2025.

(7) The Authority shall work in close cooperation with the Commissioner for Personal Data Protection when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks under Regulation (EU) 2016/679.

35(e) of 60(I) of 2025.

(8)(a) Without prejudice to legislative and institutional frameworks of the Republic, the Authority shall ensure that, in the exercise of its competences and in particular in the supervision of compliance of public administration entities with this Law and the provision and imposition of enforcement measures with regard to infringements of this Law, the Authority is functionally independent, exercises powers and carries out such tasks with operational independence vis-à-vis the public administration entities supervised.

35(e) of 60(I) of 2025.

(b) The Authority may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.

36 of 60(I) of 2025. Supervisory and enforcement measures for essential entities

36A.-(1) Supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Law shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

(2) The Authority, when exercising its supervisory tasks in relation to essential entities, shall have the power to subject those entities at least to:

(a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;

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

The targeted security audits and their frequency referred to in this paragraph shall be based on risk assessments conducted by the Authority or the audited entity, or on other risk-related available information:

The results of any targeted security audit shall be made available to the Authority, and the costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the Authority decides otherwise;

(c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Law by the essential entity;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the essential entity;

(e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 37A;

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

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor, as such qualification may be laid down in a decision of the Authority and/or of an independent auditor, and the respective underlying evidence.

(3) When exercising its powers under paragraph 2, point (e), (f) or (g), the Authority shall state the purpose of the request and specify the information requested.

(4) The Authority, when exercising its enforcement powers in relation to essential entities, shall have the power at least to:

(a) issue warnings about infringements of this Law by essential entities;

(b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or a decision requiring the entities concerned to remedy the deficiencies identified or the infringements of this Law;

(c) require the entities concerned to cease conduct that infringes this Law and desist from repeating that conduct;

(d) require the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 35 or to fulfil the reporting obligations laid down in Article 35B, in a specified manner and within a specified period;

(e) require the entities concerned to inform the natural persons or legal entities in relation to which they provide services or carry out activities that are potentially affected by a significant cyberthreat, of the nature of the threat and of any possible protective or remedial measures that can be taken by those natural persons or legal entities in response to that threat;

(f) require the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) designate a monitoring officer with clearly defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 35 and 35B;

(h) require the entities concerned to make public aspects of infringements of this Law in a specified manner;

(i) impose or request the imposition of an administrative fine pursuant to Article 43A in addition to any of the measures referred to in points (a) to (h) of this paragraph.

(5) Where enforcement measures adopted pursuant to paragraph 4, points (a) to (d) and (f), are ineffective, the Authority shall have the power to establish a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of the Authority, and if the requested action is not taken within the deadline set, the Authority shall have the power to:

(a) suspend temporarily, or request a certification or authorisation body, or

a court or tribunal, in accordance with the applicable law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity; and

(b) request that the relevant bodies, in accordance with the applicable law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity:

Temporary suspensions or prohibitions imposed pursuant to this paragraph shall be applied only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the Authority for which such enforcement measures were applied:

The imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the EU, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence:

The enforcement measures provided for in this paragraph shall not be applicable to public administration entities that are subject to this Law.

(6) Any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Law, and it is possible to hold such natural person liable for breach of its duties to ensure compliance with this Law:

As regards public administration entities, this paragraph shall be without prejudice to the applicable law as regards the liability of public servants and elected or appointed officials.

(7) When taking any of the enforcement measures referred to in paragraph 4 or 5, the Authority shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:

(a) the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event:

(i) repeated violations;

(ii) a failure to notify or remedy significant incidents;

(iii) a failure to remedy deficiencies following binding instructions from the Authority;

(iv) the obstruction of audits or monitoring activities ordered by the Authority following the finding of an infringement; and

(v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting

obligations laid down in the provisions of Articles 35 and 35B;

(b) the duration of the infringement;

(c) any relevant previous infringements by the entity concerned;

(d) any material or non-material damage caused, including any financial or economic loss, effects 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 the material or non-material damage;

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

(h) the level of cooperation of the natural persons or legal entities held responsible with the Authority.

(8)(a) The Authority shall set out a detailed reasoning for its enforcement measures and, before adopting such measures, shall notify the entities concerned of their preliminary findings, without prejudice to the provisions of Article 21.

(b) The Authority shall also allow a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.

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

(10) The Authority shall cooperate with the relevant competent authorities of the Republic pursuant to Regulation (EU) 2022/2554 and, in particular, the Authority shall inform the Oversight Forum established under Article 32(1) of Regulation (EU) 2022/2554 when exercising its supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554 with this Law:

The Authority may be informed of the designation of critical ICT third-party service providers within the Republic pursuant to Article 31(9) of Regulation (EU) 2022/2554.

36 of 60(I) of 2025. Supervisory and enforcement measures for important entities.

36B.-(1) When provided with evidence, indication or information that an important entity allegedly does not comply with this Law, in particular Articles 35 and 35B thereof, the Authority shall take action, where necessary, through ex post supervisory measures. Those measures shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

(2) The Authority, when exercising its supervisory tasks in relation to important entities, shall have the power to subject those entities at least to:

(a) on-site inspections and off-site ex post supervision conducted by trained professionals;

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

The targeted security audits referred to in point (b), shall be based on risk assessments conducted by the Authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the Authority, and the costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the Authority decides otherwise;

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

(d) requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the Authority pursuant to Article 37A;

(e) requests to access data, documents and information necessary to carry out its supervisory tasks;

(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

(3) When exercising its powers under paragraph 2, point (d), (e) or (f), the Authority shall state the purpose of the request and specify the information requested.

(4) When exercising its enforcement powers in relation to important entities, the Authority shall have the power at least to:

(a) issue warnings about infringements of this Law by the entities concerned;

(b) adopt binding instructions or a decision requiring the entities concerned to remedy the deficiencies identified or the infringement of this Law;

(c) require the entities concerned to cease conduct that infringes this Law and desist from repeating that conduct;

(d) require the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 35 or to fulfil the reporting obligations laid down in Article 35B, in a specified manner and within a

specified period;

(e) require the entities concerned to inform the natural persons or legal entities in relation to which they provide services or carry out activities that are potentially affected by a significant cyberthreat, of the nature of the threat and of any possible protective or remedial measures that can be taken by those natural persons or legal entities in response to that threat;

(f) require the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) require the entities concerned to make public aspects of infringements of this Law in a specified manner;

(h) impose or request the imposition of an administrative fine pursuant to Article 43A in addition to any of the measures referred to in points (a) to (g) of this paragraph.

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

(6) The Authority shall cooperate with the relevant competent authorities of the Republic under Regulation (EU) 2022/2554 and, in particular, the Authority shall inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising its supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554 with this Law:

The Authority may be informed of the designation of critical ICT third-party service providers within the Republic pursuant to Article 31(9) of Regulation (EU) 2022/2554.

37 of 60(I) of 2025.

PART ELEVEN

REGISTRY OF ENTITIES AND DATABASE OF DOMAIN NAME REGISTRATION DATA

Safety requirements.

37. Deleted by 38 of 60(I) of 2025.

39 of 60(I) of 2025.
Registry of entities.

37A.-(1) The Authority may submit a request to ENISA for access to the registry kept by ENISA pursuant to Article 27(1) of Directive (EU) 2022/2555.

(2) The Authority, within the scope of paragraph 4, shall require DNS service providers, TLD name 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, of online search engines and of social networking services platforms to submit the following information:

(a) the name of the entity;

Annex I.

(b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;

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 not established in the territory of the EU, the address of its representative appointed pursuant to Article 39(3);

(d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative appointed pursuant to Article 39(3);

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

(f) the entity's IP ranges.

(3) The entities referred to in the provisions of paragraph 2 shall notify the Authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three (3) months of the date of the change.

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

(5) Where applicable, the information referred to in paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 27(4).

Implementation and enforcement on a digital service provider.

38. Deleted by 40 of 60(I) of 2025.

41 of 60(I) of 2025. Database of domain name registration data.

38A.-(1) For the purpose of contributing to the security, stability and resilience of the DNS, the Authority shall require 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 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.

(2)(a) For the purposes of paragraph 1, the Authority shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

(b) Such information shall include:

(a) the domain name;

(b) the date of registration;

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

(d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

(3)(a) The Authority shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to

in paragraph 1 include accurate and complete information.

(b) The Authority shall require such policies and procedures to be made publicly available.

(4) The Authority shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

(5)(a) The Authority shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by 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 shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within seventy-two (72) hours of receipt of any requests for access.

(c) The Authority shall require policies and procedures with regard to the disclosure of such data to be made publicly available.

(6) Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data, and, to that end, TLD name registries and entities providing domain name registration services shall cooperate with each other.

42 of 60(I) of 2025. Jurisdiction and territoriality.

39.-(1) Entities falling within the scope of this Law shall be considered to fall under the jurisdiction of the Republic, except in the case of:

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

(b) DNS service providers, TLD name 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, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;

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

(2)(a) For the purposes of this Law, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken.

(b) Where such a Member State cannot be determined or where such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out.

(c) Where such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

(3)(a) Where an entity as referred to in paragraph 1, point (b), is not established in the Republic or in another Member State, but offers services within the Union, it shall designate a representative in the Union who shall be established in one of those Member States where the services are offered.

(b) Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established.

(c) In the absence of a representative in the Union designated under this paragraph, the Republic and any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Law.

(4) The designation of a representative by an entity as referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.

(5) Where the Authority receives a request for mutual assistance in relation to an entity as referred to in paragraph 1 may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on the Republic's territory.

43 of 60(I) of 2025.

PART TWELVE

PROVIDERS OF ELECTRONIC COMMUNICATIONS NETWORKS AND/OR SERVICES

44(a) of 60(I) of 2025.

Providers of electronic communications networks and/or services.

40.-(1) Deleted by 44(b) of 60(I) of 2025.

(2) Deleted by 44(b) of 60(I) of 2025.

(3) Deleted by 44(b) of 60(I) of 2025.

(4) Deleted by 44(b) of 60(I) of 2025.

(5) Deleted by 44(b) of 60(I) of 2025.

(6) This Article shall apply without prejudice to Regulation (EU) 2016/679 and the Law on the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Movement of such Data.

(7) Deleted by 44(b) of 60(I) of 2025.

(8) Deleted by 44(b) of 60(I) of 2025.

(9) Deleted by 44(b) of 60(I) of 2025.

(10) Deleted by 44(b) of 60(I) of 2025.

44(c) of 60(I) of 2025.

(11) If it is established that there is a risk of breach of the security of electronic communications networks and/or services due to the use of the service and/or if it is established that there is a risk of breach of the security of the network of an essential and/or important entity, the Authority may request the providers of electronic communications networks and/or services to take measures, including temporary and/or necessary measures, such as the termination of the service and/or the termination of access to the domain names and/or the termination of access to the internet protocol addresses, if they are used for cyberattack purposes:

Where the risk referred to in this paragraph ceases to exist or changes, the Authority may decide, as the case may be, to lift the temporary and/or necessary measures or to amend those measures.

(12) **Deleted by 44(b) of 60(I) of 2025.**

(13) **Deleted by 44(b) of 60(I) of 2025.**

45 of 60(I) of 2025.

PART THIRTEEN

STANDARDISATION, VOLUNTARY NOTIFICATION AND RADIO EQUIPMENT

46 of 60(I) of 2025. Standardisation.

41.-(1) In order to promote the convergent implementation of Article 35(1) and (2), the Authority shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and specifications relevant to the security of network and information systems.

(2) In implementing paragraph 1, the Authority shall take into account any

advice and guidelines issued by ENISA pursuant to Article 25(2) of Directive (EU) 2022/2555.

47 of 60(I) of 2025. Use of European cybersecurity certification schemes.

41A.-(1)(a) In order to demonstrate compliance with the particular requirements of Article 35, the Authority may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.

(b) Furthermore, the Authority shall encourage essential and important entities to use qualified trust services.

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

48 of 60(I) of 2025. Voluntary notification.

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

(a) essential and important entities with regard to incidents, cyberthreats and near misses; and

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

(2) The Authority shall process the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 35B, only where such processing does not constitute a disproportionate or unnecessary burden on the Authority.

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

(4) Where necessary, the Authority, as a single point of contact, shall provide information about notifications received pursuant to 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 reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

49 of 60(I) of 2025.
Radio equipment.

42A.-(1) The Authority shall ensure that radio equipment within certain categories or classes is so constructed that it complies with the essential requirements, and in particular that:

(a) it does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

(b) it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

(c) it supports certain features ensuring protection from fraud;

(d) it supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.

(2)(a) The Authority shall adopt a decision laying down the requirements to be complied with by radio equipment in order to be placed on the Cypriot market, put into service and be used, other parameters and conformity assessment procedures, as well as the criteria and procedure for the approval of notified bodies and market surveillance, including the power of seizure.

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

(3)(a) Where radio equipment presents a risk to the health or safety of persons security of networks, of information and of information systems or to other aspects of public interest protection, an evaluation shall be carried out and all necessary measures shall be taken to bring the equipment into compliance or eliminate the risk, and the Authority shall lay down in a decision the evaluation procedure and the measures that may be taken.

The Authority shall notify the Commission of any decision concerning radio equipment which does not comply with the relevant provisions of the legislation in force.

PART FOURTEEN
PENALTIES

Administrative fine. 50(a) of 60(I) of 2025.

43.-(1) Without prejudice to Article 43A, where the Authority finds that a person has committed an act or has omitted to act in breach of the provisions of this Law, it may impose an administrative fine not exceeding two hundred thousand euro (EUR 200 000), depending on the seriousness of the infringement, and, if the infringement is repeated, a fine not exceeding ten thousand euro (EUR 10 000) for each day that the infringement continues.

The procedure for imposing the administrative fine shall be laid down in a decision of the Authority.

(2) The Authority may impose an administrative fine on any person who commits an act or omits to act in breach of the provisions of any decisions and/or regulations of the European Union, which shall not exceed three hundred thousand four hundred euro (EUR 300 400) and, if the infringement is repeated, an administrative fine not exceeding two hundred thousand euro (EUR 200 000).

50(b) of 60(I) of 2025.

(3) The Authority may issue decisions on the procedure for imposing administrative fines and/or other administrative penalties for non-compliance with this Law and/or decisions of the Authority and/or regulations of the European Union, within the meaning given to the terms in the Implementation of European Community regulations and European Community Decisions Law of 2007, and may determine the amount of those fines and penalties and the procedure for imposing them by a decision.

50(c) of 60(I) of 2025.

(4) Before the Authority imposes an administrative fine, shall notify the affected person of its intention to impose an administrative fine, by informing such person of the reasons why it intends to do so and giving him the right to submit representations, within ten (10) working days from the day of the notice.

50(d) of 60(I) of 2025.

(5) The Authority shall impose an administrative fine under the provisions of paragraph 1 by means of a written and reasoned decision, which it shall forward to the affected person by registered letter, specifying the infringement and informing the affected person:

131(I) of 2015 and 72(I) of 2018.

(a) on his right to challenge the decision by recourse to the Administrative Court, in accordance with Article 146 of the Constitution and the Law on the Establishment and Operation of an Administrative Court of 2015; and

(b) the period within which the aforementioned right may be exercised.

(6) If a person on whom an administrative fine has been imposed under the provisions of this Law refuses or fails to pay the said fine to the Authority, the Authority shall initiate court proceedings and shall collect the amounts due as a civil debt owed to the Republic.

51 of 60(I) of 2025. Imposing administrative fines on essential and important entities.

43A.-(1) The administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Law shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

(2) Administrative fines shall be imposed in addition to any of the measures referred to in Article 36A(4), points (a) to (h), Article 36A(5) and Article 36B(4), points (a) to (g).

(3) When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the

provisions of Article 36A(7).

(4) Where they infringe Article 35 or 35B of this Law, essential entities shall be subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least ten million euro (EUR 10 000 000) or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

(5) Where they infringe Article 35 or 35B, important entities shall be subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least seven million euro (EUR 7 000 000) or of a maximum of at least 1.4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

(6) The Authority may, by a decision, provide for other administrative penalties to be imposed in order to compel an essential or important entity to cease an infringement of this Law in accordance with a prior decision of it.

Criminal offences. 52(a)(i)(ii)(iii)(iv) of 60(I) of 2025.

44.-(1) An essential and/or important entity that fails to notify the Authority, without undue delay, of an incident that has a severe impact on the continuity of its essential services shall be guilty of an offence and, if convicted, shall be liable to imprisonment for a term not exceeding two (2) years or a fine not exceeding ten thousand euro (EUR 10 000) or to both such penalties.

(2) Deleted by 52(b) of 60(I)/2025.

52(c)(i)(ii)(iii) of 60(I) of 2025.

(3) An essential and/or important entity that fails to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of networks and information systems which it uses for its operations shall be guilty of an offence, and if convicted, shall be liable to imprisonment for a term not exceeding three (3) years or a fine not exceeding fifteen thousand euro (EUR 15 000) or to both such penalties.

(4) **Deleted by 52(b) of 60(I) of 2025.**

(5) Any person who fails to provide any information requested by the Authority, in accordance with Article 20(1)(b), within fifteen (15) days of the date of the request shall be guilty of an offence and, if convicted, shall be liable to imprisonment for a term not exceeding three (3) years or a fine not exceeding three thousand four hundred euro (EUR 3 400).

(6) Any person required by the Authority to provide any information, in accordance with the relevant provisions of regulations issued by the European Union, and who fails to do so within the specified period of fifteen (15) days of the date of the request, shall be guilty of an offence and, if convicted, shall be liable to imprisonment for a term not exceeding six (6) months or to a fine not exceeding three thousand four hundred euro EUR 3 400 or to both such penalties.

(7) Any person who violates any provision of the decisions and/or regulations of the European Union on the security of networks and information systems shall be guilty of an offence, and if convicted, shall be liable to imprisonment for a term not exceeding three (3) years or a fine not exceeding fifteen thousand euro (EUR 15 000) or to both such penalties.

53 of 60(I) of 2025. Infringements

44A.-(1) Where the Authority becomes aware in the course of supervision or

entailing a personal data breach.

enforcement actions that the infringement by an essential or important entity of the obligations laid down in Articles 35 and 35B of this Law may entail a personal data breach, as defined in Article 4(12) of Regulation (EU) 2016/679 and which is to be notified pursuant to Article 33 of that Regulation, it shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation.

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

(b) The Authority may, however, impose the enforcement measures provided for in Article 36A(4)(a) to (h), Article 36A(5) and Article 36B(4)(a) to (g) of this Law.

(3) Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the Authority, the Authority shall inform the Commissioner for Personal Data Protection of the potential data breach referred to in paragraph 1.

PART FIFTEEN REGULATIONS, DECISIONS, FINANCIAL PROVISIONS, REPORTS AND VARIOUS OTHER MATTERS

Adoption of Regulations.

45.-(1) For the better implementation of the provisions of this Law, the Council of Ministers shall adopt regulations, to be submitted to the House of Representatives for approval and published in the Official Gazette of the Republic, unless otherwise provided therein.

(2) Without prejudice to the generality of the provisions of paragraph 1, these regulations may provide, inter alia, for the following:

(a) The methodology for calculating fees to finance the Authority's costs;

(b) the procedure for the appointment, either permanently or by contract for a specified period of time, for the promotion, the terms of service, the categories of posts, the retirement and retirement benefits of the members of staff of the Authority, as well as the disciplinary code and the exercise of disciplinary control;

(c) the schemes of service concerning the duties, responsibilities and qualifications of the Authority's permanent staff;

(d) the Healthcare Fund to cover the Authority's staff members during and after their service with the Authority in accordance with the Regulation on Electronic Communications and Postal Regulation (Healthcare Fund) Regulations and the provisions of the General Healthcare System Law; Healthcare Fund to cover staff members of the Authority during and after their service with the Authority in accordance with the Law on the Regulation of Electronic Communications and Postal Services and the provisions of the General Healthcare System Law;

(e) the Provident Fund for the employees of the Authority during their service with the Authority;

(f) the Provident Fund for Hourly Paid Personnel for hourly paid members of staff

of the Authority.

Adoption of decisions by the Authority.

46.-(1) For the better implementation of the provisions of this Law, the Authority shall issue decisions in the exercise of its functions under the provisions of this Law.

(2) Without prejudice to the generality of the provisions of paragraph 1, the Authority may adopt decisions aimed primarily at clarifying and regulating the procedures, methods, timetables and in particular the procedure and manner for the collection of all amounts, fees and charges which are payable under the provisions of this Law and the decisions made thereunder, the procedure and manner of collection of all amounts of administrative fines which are payable and any other revenue that is payable or any amounts which are collected under the provisions of this Law and the decisions made thereunder, the determination of fees and levies which are payable in connection with the implementation of the provisions of this Law and the decisions made thereunder and the determination of a procedure for the imposition of an administrative fine.

(3) The Authority may issue decisions regarding the application of best practices or guidelines issued by the Commission concerning the application of Union law.

(4) The Authority may issue decisions regarding any other matter referred to in the provisions of this Law or required or which needs to be regulated.

(5) The decisions of the Authority made under this Law shall be published in the Official Gazette of the Republic and shall enter into force at a time specified in the relevant decision or, in the absence of a fixed date of entry into force, from the date of such publication of the relevant decision:

Decisions concerning sensitive and/or confidential information and/or classified documents shall not be published in the Official Gazette of the Republic.

(6) The Authority shall have the power to implement, by means of a decision, the regulations of the European Union relating to the security of networks and information systems and cybersecurity.

Budget.

47.-(1) The Authority shall prepare a revenue and expenditure budget for each financial year, beginning on 1 January and ending on 31 December.

54 of 60(I) of 2025.

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

(b) After approval of the budget by the Council of Ministers, it shall be submitted to the House of Representatives for approval in accordance with Article 104 of the Fiscal Responsibility and Financial Framework Law.

(3) The budget, following any amendments made by the Council of Ministers, shall be submitted to the House of Representatives before 30 September each year.

(4) The budget shall cover the Authority's financial programme for each financial year, which starts on 1 January and ends on 31 December:

The Authority's first financial programme shall start from the date of operation of the Authority and end on 31 December of the same year.

(5) The manner in which the budget shall be prepared and the manner in which the

breakdown of funds will be shown in the revenue and expenditure table shall be similar to the manner in which the state budget is drawn up.

(6) The Authority shall ensure the preparation of a budget as referred to in the provisions of paragraph 1 and the preparation of a financial plan as referred to in the provisions of paragraph 4.

(7) If the budget is not adopted in due time, the Authority shall operate in accordance with Article 168(3) of the Constitution concerning the State budget, with the 'twelfths' system taking effect.

Bookkeeping.

48.-(1) The Authority shall keep appropriate books and accounts for its activities, as determined by the Auditor-General of the Republic.

(2) Regarding the financial management of each financial year, the Authority shall ensure that a report is drawn up in a manner to be determined by the Auditor-General of the Republic.

(3) The accounts of the Authority shall be audited by the Auditor-General of the Republic.

(4) Within one month of the audit of the accounts, the Authority shall submit a financial management report to the Council of Ministers and the House of Representatives for information purposes.

(5) The Authority shall ensure that books and accounts are kept and a report is drawn up in accordance with paragraphs 1, 2 and 4.

Report.

49.-(1) The Authority shall submit a report on its activities to the President of the Republic on an annual basis within six (6) months of the end date of each financial year.

(2) the Authority shall communicate its report to the Council of Ministers and to the House of Representatives and may publish it.

Employment of staff, in case the Authority ceases to exist.

50. If the Authority ceases to exist for any reason, the permanent staff posts and the staff filling those posts and any vacant posts shall be transferred to an appropriate ministry, department or agency, and if the Authority's functions, powers and duties under the provisions of this Law are transferred for any reason to another legal entity, authority or organisation, the staff of the Authority shall provide services to that legal entity, authority or body without any change in their status or in their terms of service.

Assets belonging to the Authority, in case it ceases to exist.

51. If the Authority ceases to exist for any reason, all the Authority's assets shall devolve upon the Republic.

Recourse to the Administrative Court against decisions of the Authority.

52.-(1) Any decision of the Authority shall be subject to judicial review by appeal to the Administrative Court in accordance with Article 146 of the Constitution and the Law on the Establishment and Operation of an Administrative Court.

(2) The Authority shall keep a record of appeals, the duration of appeal procedures and the number of decisions to grant interim measures and shall provide that information to the Commission or another institution of the European Union upon a reasoned request.

Liability of the

53. Subject to the provisions of this Law and the regulations and decisions adopted

Commissioner, of the Deputy Commissioner and of the staff of the Authority.

thereunder, the Commissioner, Deputy Commissioner and the members of the staff of the Authority shall not be liable for anything done or omitted to be done or said or for any opinion expressed or report or other document prepared in good faith in the exercise of their respective duties and responsibilities and powers under the provisions of this Law.

Liability of legal entities.

54. (1) A legal entity shall be guilty of an offence pursuant to Articles 22 and 43 where the offence is committed for the benefit of the legal entity by any person acting either individually or as part of an organ of that entity and holding a leading position within it as:

(a) an authorised representative of the legal entity;

(b) a proxy holder authorised to take decisions on behalf of the legal entity; or

(c) a proxy holder authorised to exercise control within the legal entity.

(2) A legal entity shall be guilty of an offence pursuant to Articles 22 and 43, where the lack of supervision or control by a person specified in the provisions of paragraph 1 has enabled the commission of that offence for the benefit of the legal entity by a person acting under the authority of the person specified in the provisions of paragraph 1.

(3) Without prejudice to the provisions of paragraphs 1 and 2, the liability of the legal entity shall not exclude the initiation of criminal proceedings against the natural persons who commit the offences and/or the persons involved in the commission of the offences referred to in Articles 22 and 43.

(4) Without prejudice to the provisions of paragraphs 1 and 2, a person who advises, promotes or induces another person to participate in the commission or attempted commission of an offence pursuant to Articles 22 and 43 shall be guilty of an offence of the same type, shall be subject to the same penalty and may be prosecuted as if they had committed such an act themselves.

(5) In the event of an act or omission on the part of a legal entity which leads to the imposition of an administrative fine or of any other pecuniary fine by the Authority, in accordance with the provisions of this Law and/or the decisions made thereunder, the legal entity and the natural persons referred to in the provisions of paragraph 1 shall be liable for the act or omission and for the payment of the administrative fine.

PART SIXTEEN
TRANSITIONAL AND FINAL PROVISIONS

Transitional provision.

55.-(1) Decisions or regulations adopted pursuant to the Security of Networks and Information Systems Law of 2018, which is repealed by this Law, as well as notifications made to the Commission shall be deemed to have been made under the provisions of this Law and shall remain in force until repealed or replaced by decisions, regulations and/or notifications to the Commission, as the case may be, to be adopted under the provisions of this Law.

(2) Any reference to 'OCECPR' in the relevant legislation or in regulations or orders issued thereunder or in relevant public documents relating to issues regarding the security of networks and information systems, shall be deemed to be

a reference to the 'Authority'.

55 of 60(I) of 2025.

(3) Decisions or regulations adopted pursuant to the Security of Networks and Information Systems Law of 2020 shall remain in force until repealed or replaced by decisions and/or regulations adopted under the provisions of this Law or in the context of the fulfilment of EU obligations, as the case may be.

(4) Upon the entry into force of a law that provides for the consolidation of the Authority with the OCECPR, amendments will be made to the Authority's structure, administration, operation, staff matters, financial management and budget. Specifically, Articles 4 to 14, Article 45(2), points (b) to (f), Article 47, Article 50 and Article 53 of the Security of Networks and Information Systems Law are expected to be amended or repealed accordingly.

Repeal. 17(I) of 2018.

56. From the date of publication of this Law in the Official Gazette of the Republic, the Security of Networks and Information Systems Law of 2018 shall be repealed.

57 of 60(I) of 2025. Entry into force **60(I)/2025**

57.-(1) Without prejudice to paragraph 2, this Law **[60(I)/2025]** shall enter into force on the date of its publication in the Official Gazette of the Republic.

Correction O.G., Annex I(I), No 5043, p. 489

(2) The provisions of Article 8 of this Law **[60(I)/2025]** shall enter into force on a date set by the Council of Ministers in a notice published in the Official Gazette of the Republic.

56 of 60(I) of 2025

TABLE
(Article 56)

ANNEX I
(Articles 2A and 27)

SECTORS OF HIGH CRITICALITY

	Sector	Subsector	Type of entity
1.	Energy	(a) Electricity	— Electricity undertakings as defined under the provisions of the Law Regulating the Electricity Market, which carry out the function of 'supply', as defined under the provisions of that same Law — Distribution system operators as defined under the provisions of the Law Regulating the Electricity Market — Transmission system operator Cyprus as defined in the provisions of the Law Regulating the Electricity Market — Producers as defined under the provisions of the Law Regulating the Electricity Market — Nominated electricity market operators as defined 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 for electricity. — Market participants as defined in Article 2(25) of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services, as defined under the provisions of the Law Regulating the Electricity Market — Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
		(b) District heating and cooling	— Operators of district heating or district cooling as defined in the provisions of the Law Regulating the Electricity Market
		(c) Oil	— Operators of oil transmission pipelines — Operators of oil production, refining and treatment facilities, storage and transmission — Central stockholding entities as defined under the provisions of the Petroleum Products Stocks Conservation Law
		(d) Gas	— Supply undertakings as defined under the provisions of the Natural Gas Market Regulation Law — Distribution system operators as defined under the provisions of the Law Regulating the Electricity Market — Transmission system operators as defined under the provisions of the Natural Gas Market Regulation Law — Storage system operators as defined under the

			provisions of the Natural Gas Market Regulation Law — LNG system operators as defined under the provisions of the Natural Gas Market Regulation Law — Natural gas undertakings as defined under the provisions of the Natural Gas Market Regulation Law — Operators of natural gas refining and treatment facilities
		(e) Hydrogen	— Operators of hydrogen production, storage and transmission
2.	Transport	(a) Air	— Air carriers shall have the meaning given to this term in Article 3(4) of Regulation (EC) No 300/2008, used for commercial purposes — Airport managing bodies as defined under the provisions of the Civil Aviation Law, and airports as defined under the provisions of the Civil Aviation Law, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council, and entities operating ancillary installations contained within airports — Traffic management control operators providing air traffic control (ATC) services as defined in Article 2(1) of Regulation (EC) No 549/2004 of the European Parliament and of the Council
		(b) Rail	— 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 under the provisions of the Railway Undertakings Licensing Law, including operators of service facilities as defined in Article 3(12) of Directive 2012/34/EU
		(c) Water	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council, not including the individual vessels operated by those companies — Managing bodies of ports as defined under the provisions of the Enhancing of Port Security Law, including their port facilities as defined in Article 2(11) of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports — Operators of vessel traffic services (VTS), as defined under the provisions of the Merchant Shipping (Community Vessel Traffic Monitoring and Information System) Law
		(d) Road	— Road authorities within the meaning given to this term by Article 2(12) of Commission Delegated Regulation (EU) 2015/962, responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent

[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. 6).

		transport systems is a non-essential part of their general activity — Operators of intelligent transport systems as defined under the provisions of the Law on the Framework for the Deployment of Intelligent Transport Systems in the field of Road Transport and Interfaces with other Modes of Transport
3.	Banking	— Credit institutions within the meaning given 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 infrastructure	— Operators of trading venues as defined under the provisions of the Law on Investment Services, Activities and Regulated Markets — Central counterparties (CCPs) within the meaning given to this term in Article 2(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 under the provisions of the Law on the Application of Patients' rights in Cross-border Healthcare — 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 of medicinal products as defined 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 to be critical during a public health emergency (public health emergency critical devices list) within the meaning given to this term in Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices
6.	Drinking water	Suppliers and distributors of water intended for human consumption as defined in the Law on the Quality of Water intended for Human Consumption, excluding distributors for which distribution of water for human consumption is a non-essential part of their general

		activity of distributing other commodities and goods
7.	Waste water	Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined under the provisions of the Integrated Water Management Law, excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity.
8.	Digital infrastructure	— Internet Exchange Point providers — DNS service providers excluding operators of root name servers — TLD name registries — Cloud computing service providers — Data centre service providers — Content delivery network providers — Trust service providers — Providers of public electronic communications networks — Providers of publicly available electronic communications services
9.	ICT service management (business-to-business)	— Managed service providers — Managed security service providers
10.	Public administration	— Public administration entities of central governments — Public administration entities of the wider public sector
11.	Space	Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

56 of 60(I) of 2025

ANNEX II
(Articles 2A and 27)

OTHER CRITICAL SECTORS

	Sector	Subsector	Type of entity
1.	Postal and courier services		Postal service providers as defined under the provisions of the Law on the Regulation of Electronic Communications and Postal Services, including providers of courier services.
2.	Waste management		Undertakings carrying out waste management as defined under the provisions of the Waste Law, excluding undertakings for whom waste management is not their principal economic activity.
3.	Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3(9) and (14) of Regulation (EC) No 1907/2006 of the European Parliament and of the Council and undertakings that produce articles, as defined in Article 3(3) of that Regulation, from substances or mixtures
4.	Production, processing and distribution of food		Food businesses, as defined in Article 3(2) of Regulation (EC) No 178/2002 of the European Parliament and of the Council, engaged in wholesale distribution and industrial production and processing.
5.	Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices as defined in Article 2(1) of Regulation (EU) 2017/745 of the European Parliament and of the Council, and entities manufacturing in vitro diagnostic medical devices as defined in Article 2(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 Annex I, point 5, fifth indent, of this Directive.
		(b) Manufacture of computer, electronic and optical products	|Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
		(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
		(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
		(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
		(f) Manufacture of other transport	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE

	equipment	Rev. 2
6.	Digital providers	— Providers of online marketplaces — Providers of online search engines — Providers of social networking services platforms
7.	Research	Research organisations