Preamble. Official Journal Of the EU: L194, 19.7.2016, p.1.	**Number 89(I) of 2020** THE SECURITY OF NETWORKS AND INFORMATION SYSTEMS LAW ,2020 For the purposes of harmonisation with the act of the European Union with title 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union',
Short Title.	1. This Law may be cited as the Security of Networks and Information Systems Law,2020.
	PART ONE GENERAL – INTERPRETATIVE PROVISIONS
Exclusions from the scope of application. Official Journal of the EU: L257, 28.8.2014, p. 73.	**2**.-(1) The security and notification requirements provided by this Law shall not apply to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
	(2) This Law shall be without prejudice to the actions taken by the Republic to safeguard its essential State functions and in particular to safeguard national security, including actions protecting information the disclosure of which it considers contrary to the essential interests of its security, as well

	as to maintain law and order and in particular to facilitate the investigation, detection and prosecution of criminal offences.
91(I) of 2014 105(I) of 2014. 147(I) of 2015. Official Gazette, Third Supplement (I): 20.01.2012.	(3) This Law shall apply without prejudice to the Prevention and Combating of Sexual Abuse, Sexual Exploitation of Children and Child Pornography Law, the Attacks Against Information Systems Law and the Identification and Designation of the European Critical Infrastructures and the Assessment of the Need to Improve their Protection Regulations.
Interpretation.	**3**.-(1) In this Law, unless the context otherwise requires:
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	“representative” means any natural or legal person established in the European Union and explicitly designated to act on behalf of a digital service provider not established in the European Union, which may be addressed by a national competent authority or the CSIRT, instead of the digital service provider, with regard to its obligations under Directive 2016/1148/EU; "Authority" means the Digital Security Authority; “security of network and information systems” means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems; "Deputy Commissioner" means the Deputy Commissioner of Communications appointed under the provisions of subsection (2) of section 5 of the Electronic Communications and Postal Regulation Law, who advises and assists the Commissioner in the exercise of his functions, powers and duties provided by this Law and performs any other duties assigned to him under this Law; "Office" or "OCECPR" means the Office of the Commissioner of Electronic Communications and Postal Regulation, established under the provisions of subsection (1) of section 10 of the Electronic Communications and Postal Regulation Law;

160(I) of 2013 77(I) of 2014 104(I) of 2016 112(I) of 2016 76 (I) of 2017.	''Republic'' means the Republic of Cyprus; “network and information system” means: (a) an electronic communications network as defined in the provisions of subsection (1) of section 4 of the Electronic Communications and Postal Regulation Law, or (b) any device or group of interconnected or related devices one or more of which, pursuant to a program, perform automatic processing of digital data, or (c) digital data stored, processed, retrieved or transmitted by elements covered by the provisions of paragraphs (a) and (b) for the purposes of their operation, use, protection and maintenance; “national strategy on the security of network and information systems and cybersecurity” means the framework providing strategic objectives and priorities on the security of network and information systems and cybersecurity at national level; “national CSIRT” means the national emergency response body to incidents related to the security of network and information systems;

85(I) of 2017.	“online marketplace” means a digital service that allows consumers and/or traders as respectively defined in section 2 of the Alternative Resolution of Consumer Disputes Law, to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace; “online search engine” means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found; ''Commissioner'' means the Commissioner of Communications appointed under the provisions of subsection (1) of section 5 of the Electronic Communications and Postal Regulation Law; 'Commission' means the Commission of the European Union;

	'ENISA' means the European Union Agency for Network and Information Security;
Official Journal of the EU: L316, 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: L119, 04.05.2016, 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; “risk” means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems; "Central Bank" means the Central Bank of Cyprus; "critical infrastructure" means the assets, systems or parts thereof located within the Republic, which are essential for the maintenance of vital functions of society, the health, safety, economic and social well-being of its members and whose disruption or destruction would have a significant impact on the Republic, as a result of the inability to maintain these functions; “critical information infrastructure” means network and information systems which are by their nature critical infrastructures or are necessary for the operation of other critical infrastructures; “top-level domain name registry” means the entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD); "Directive (EU) 2016/1148" means Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;

	"electronic communications network provider" means a person authorised by the Commissioner to provide a public electronic communications network under the Electronic Communications and Postal Regulation Law; "provider of electronic communications services" means a person authorised by the Commissioner to provide publicly available electronic communications services under the Electronic Communications and Postal Regulation Law; 'domain name system service provider' means an entity that provides domain name system services on the internet; 'digital service provider' means any legal person providing a digital service; 'specification' means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012; "head" means the person who holds the hierarchically highest post in the Authority and who is subordinate to the Commissioner; "standard" means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012; 'Internet Exchange Point' or 'IXP' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic; 'incident' means any event having an actual adverse effect on the security of network and information systems; 'Advisory Committee' has the meaning assigned to this term by the provisions of section 32 of the Electronic Communications and Postal Regulation Law; 'Domain Name System or 'DNS' means a hierarchical distributed naming system in a network which refers queries for domain names; 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources;

	"Deputy Minister" means the Deputy Minister of Research, Innovation and Digital Policy next to the President; 'operator of essential services' means the public or private entity of a type referred to in a Decision adopted by the Authority which meets the criteria laid down in the provisions of subsection (2) of section 27; 'operator of critical information infrastructures' means the body administering critical information infrastructures referred to in a Decision of the Authority; 'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto;
Official Journal of the EU: L241, 17.09.2015, p. 1.	'digital service' means a service within the meaning of Article 1(1) of Directive (EU) 2015/1535 of the European 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, which is of a type set out in a Decision adopted by the Authority;
	(2) Any terms used in this Law and not otherwise defined shall have the meaning assigned to them by the Electronic Communications and Postal Regulation Law.
	PART TWO APPOINTMENT AND DISMISSAL OF THE COMMISSIONER AND DEPUTY COMMISSIONER OF COMMUNICATIONS
Appointment and dismissal of the Commissioner and of the Deputy Commissioner of Communications.	**4.** For the appointment and dismissal of the Commissioner of Communications and of the Deputy Commissioner of Communications, in relation to the performance of their duties under the provisions of this Law, the provisions of sections 5 to 7 of the Electronic Communications and Postal Regulation Law shall apply.

Remuneration and obligations of the Commissioner of Communications and of the Deputy Commissioner **of** Communications.	**5**. The provisions of sections 8 to 9 of the Electronic Communications and Postal Regulation Law shall apply to the remuneration and obligations of the Commissioner of Communications and of the Deputy Commissioner of Communications, as well as their obligations after retirement.
	PART THREE DIGITAL SECURITY AUTHORITY
National competent authority for the security of network and information systems and cyber-security. 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 the provisions of section 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 in the provisions of 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, as the Commissioner himself may decide, and perform any other duties assigned to him under this Law. (b) In case of removal or resignation of the Commissioner in accordance with the provisions of section 6 of the Electronic Communications and Postal Regulation Law, death, permanent absence or other permanent impediment to the exercise of his functions, powers and duties under the provisions of the Electronic Communications and Postal Regulation Law and/or this Law, the functions, powers and duties of the Commissioner assigned to him under the provisions of this Law shall be exercised temporarily by the Deputy Commissioner until another Commissioner is appointed, as provided in the Electronic Communications and Postal Regulation Law. (c) In case of 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 the provisions of subsection (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 the provisions of subsection (3) of section 3 of the Security of Networks and Information Systems Law, 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. (4) The Authority shall continue to be staffed, operated and administered in accordance with this Law 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 for the fulfilment of 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 take all necessary actions to ensure that the financial and human resources at its disposal are sufficient to carry out the tasks entrusted thereto. (8) In the performance of its duties, the Authority shall apply the relevant legislation concerning secret and confidential information which it handles. (9) The national CSIRT, which shall form part of the Authority in accordance with the provisions of subsection (8) of section 3 of the Security of Networks and Information Systems Law, 2018, shall continue to receive instructions and guidance from the Authority and shall be under its supervision.
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 its operation needs; (b) 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 a public or other provider of electronic communications network or services or an operator of essential services or an operator of critical information infrastructure or a digital service provider 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 provider, entity, or electronic communications undertakings;

20(I) of 2014 123(I) of 2016 133(I) of 2016 159(I) of 2017.	(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; (e) make loans which are necessary for the implementation of all provisions included in paragraphs (a), (c) and (d), in compliance with the provisions of section 103 of the Fiscal Responsibility and Financial Framework Law, (f) receive, subject to the provisions of this section and section 8, and manage all amounts paid under the provisions of this Law or the decisions or regulations made thereunder; (g) conclude contracts, and (h) do anything required to fulfil the provisions of this section.
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 in the provisions of this Law and/or the Decisions and/or provisions of the Regulations made thereunder, (b) any grant provided to the Authority under the provisions of paragraph (b) of section 7 and any other income received under this Law; (c) all revenues derived from the Authority's assets in accordance with the provisions of section 7; (d) all amounts of salaries, emoluments, benefits, pensions, remuneration and hire of services paid by the Republic to the Authority, in accordance with the provisions of subsection (1) of section 11, for payment by the Authority to its members of staff or to persons with whom it has concluded service contracts pursuant to the provisions of section 14, as the case may be.

Staff of the Authority.	**9**.-(1) For the appointments and promotions of the staff of the Authority, there shall be established a three -member Board, referred to as the "Selection and Promotions Council of the Digital Security Authority" (hereinafter the SPCA) and shall comprise of: (a) The Commissioner, as chairman, (b) the Deputy Commissioner, and (c) the Chairman of the Advisory Committee, appointed under the provisions of paragraph (b) of subsection (1) of section 32 of the Electronic Communications and Postal Regulation Law and, in case of his impediment, he shall be substituted by one of the two members of the Advisory Committee who are 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 certain period of time in accordance with the relevant procedures as laid down in Regulations made pursuant to the provisions of section 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 made pursuant to the provisions of section 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 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. (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 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 the 1st , October 2011, as well as the benefits and pensions of dependents of such members and of the families of such members.

Official Gazette, Third Supplement(I): 23.02.2007. 89(I) of 2001 134(I) of 2002 101(I) of 2004 62(I) of 2005 74(I) of 2017 25(I) of 2020.	(c) Without prejudice to the provisions of paragraph (b), Regulations made pursuant to the provisions of section 45 may prescribe, regulate and provide for the establishment of- (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 dependents of these members, which will operate in accordance with the provisions of the Commissioner of Electronic Communications and Postal Regulation (Health Care Fund) Regulations and the provisions of the General Health System Law; (ii) a Provident Fund to cover the employees of the Authority during their service with the Authority; (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 schemes of service drawn up by the Commissioner by Regulations, which shall be issued in accordance with the provisions of section 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 under the provisions of subsection (1) of section 9. (2) The disciplinary offences, the modus operandi of the SPCA for the purposes of disciplinary control, as well as the provisions and procedures under which it exercises disciplinary control over the staff of the Authority shall be determined by Regulations made in accordance with the provisions of section 45.

Financing of the Authority's expenditure.	**11**.-(1)(a) The Authority shall be financed by operators of essential services and operators of critical information infrastructure, providers of digital services and providers of electronic communications networks and/or services, as specified in Regulations made pursuant to the provisions of section 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 under the provisions of section 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 the provisions of subsection (1) shall be repayable to the Republic and shall be paid by the Authority without delay: Provided that the Republic shall not proceed to 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.**There shall be paid from the Authority's Fund: (a) To the Republic all sums repayable to it under the provisions of subsection (2) of section 11, (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 the provisions of

	paragraph (b) of subsection (4) of section 9, to the dependants and families of such members, as well as all amounts of remuneration payable under service contracts which are concluded by the Authority under the provisions of section 14, as well as all amounts of contributions payable to the funds referred to in the provisions of paragraph (c) of subsection (4) of section 9, as provided in Regulations made pursuant to section 45; (d) all costs incurred in any appointment of an advisory body under the provisions of section 25; (e) the amortisation of any loan concluded by the Authority under the provisions of paragraph (e) of section 7; (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, (j)all moneys that the Authority is obliged to pay in the exercise of its functions under this Law, as damages pursuant to any court decisions or out-of-court settlements, to the Consolidated Fund of the Republic.
Obtaining of services by the Authority. 173(I) of 2011.	**14.** Notwithstanding the provisions of any other law, Regulations, Orders and Decisions made under any relevant legislation, the Authority may: (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,

73(I) of 2016.	(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, (c) Obtain services under hire for a specific period of time from natural or legal persons in accordance with the provisions of the Regulation of Public Procurement Procedures and Related Matters Law.
	PART FOUR GENERAL DUTIES OF THE AUTHORITY
Obligation to promote certain objectives of the Authority.	**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 achievement of a level of security of networks and information systems, including all essential services/critical information infrastructures of the Republic and digital services under the Authority's competence. (2) The Authority shall promote the maintenance of the integrity and security of electronic communications networks and information security, including the protection of critical information infrastructures. (3) With regard to matters falling within the fields of defence and security of the Republic, the Authority shall comply with instructions and/or Decisions of the Council of Ministers.
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 subsection (2). (2) The Deputy Minister, following meetings and consultations with the Commissioner as head of the Authority, shall define 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) advise the Minister on issues relating to the security of networks and information systems, digital security and cybersecurity in the Republic; (b) implement, in matters of security of networks and information systems, the general policy framework to be followed in accordance with the provisions of subsection (2) of section 16; (c) be a national single point of contact for the security of networks and information systems (hereinafter referred to as the 'single point of contact'); (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 and the network of CSIRTs, as provided for in section 33; (e) consult and cooperate with the competent law enforcement authorities and the Commissioner for the Protection of Personal Data; (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 the provisions of subsections (3), and (5) of section 35 and the provisions of subsections (3) and (6) of section 37, (g) ensure that it has sufficient resources for the effective performance of its duties and of the duties of the national CSIRT described in the provisions of paragraph (a) of subsection (2) of section 31; (h) ensure the effective, efficient and secure cooperation of the national CSIRT within the framework of the network of CSIRT referred to in section 33; (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;

	(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) inform the Commission of the mandate, as well as of the key elements of the incident handling process by the national CSIRT; (l)supervise the national CSIRT, the governmental CSIRT, the academic CSIRT or other sectoral CSIRTs in the Republic: Provided that 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; (m)ensure that the national CSIRTs have access to an appropriate, secure and resilient communication and information infrastructure at national level; (n) identify for each sector and subsector referred to in a Decision issued by the Authority the operators of essential services established in the Republic; (o) review and, where necessary, update the list of identified operators of essential services on a regular basis, at least every two years, and update the relevant list of operators of critical information infrastructure at least every two (2) years; (p) cooperate closely with the Commissioner for the Protection of Personal Data to deal with incidents leading to personal data breaches; (q) assess the compliance of operators of essential services and/or operators of critical information infrastructure with their obligations under section 35 and their impact on the security of their networks and information systems; (r) ensure that operators of essential services and/or operators of critical information infrastructure 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;

	(s) ensure that operators of essential services and/or operators of critical information infrastructure take appropriate measures to prevent and minimise the impact of incidents that affect the security of the networks and information systems which are used to provide these essential services, with a view to ensuring their continuity; (t) ensure that operators of essential services and/or operators of critical information infrastructures notify it without undue delay of incidents that have a serious impact on the continuity of the essential services they provide; (u) ensure that providers of public networks or publicly available electronic communications services notify it of any breach of security measures or loss of integrity of their networks which had a substantial impact on the functioning of their networks or services; (v) ensure that digital service providers identify and 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 the context of the provision of services referred to in a Decision made by the Authority; (w) ensure that digital service providers take measures to prevent and minimise the impact of incidents that affect the security of networks and information systems in relation to the services referred to in a Decision issued by the Authority and offered within the European Union, with a view to ensuring their continuity; (x) ensure that digital service providers notify to it, without undue delay, of any incident that has a significant impact on the provision of the service that they offer within the European Union, as set out in a Decision made by the Authority; (y) issue any Decision, including interim measures, in respect of matters falling within its functions; (z) impose an administrative fine, in accordance with the provisions of section 43, to 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 organizations in the interest of the Republic; (bb)request, in the context of its specific activities, the provision by operators of essential services and/or operators of critical information infrastructure, from digital service providers and from

125(I)of2018.	providers of electronic communications networks and/or services, any relevant technical, financial and other information, 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; (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, (ee)adopt and/or maintain provisions aimed at achieving a higher level of security of networks and information systems, without prejudice to the provisions of subsection (13) of section 37 and the obligations of the Republic deriving from Union law; (ff) subject to the provisions of subsection (3) of section 19, publish information and documents referred to in the provisions of section 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: Provided that 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; (hh)conclude memoranda of understanding with bodies governed by this Law or other authorities or organizations or companies that cooperate with the Authority; (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 to such memoranda of cooperation and/or agreements, it may be specified how the provisions implied by the designation of authorised institutions as operators of essential services or operators of critical information infrastructures are to be applied or otherwise.
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: (a) the digital service providers to provide it with the necessary information for the assessment of the security of their networks and information systems, including documented security policies, and to remedy any failure to comply, and the said requested information shall be used and maintained by the Authority in order to ensure the compliance of the digital service providers with their obligations under the provisions of this Law, the provisions of the Regulations made thereunder and the provisions of the Decisions of the Authority made for the implementation of the provisions of this Law, (b) the operators of essential services and/or the operators of critical information infrastructure, 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 operators of essential services and/or operators of critical information

	infrastructure 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 the provisions of this Law, (c) the providers of electronic communications networks and/or services, information that is used and maintained in order to ensure their compliance with their obligations under the provisions of this Law, the provisions of the Regulations and Decisions made for the implementation of the provisions of this Law as well as information which is necessary for the investigation and management of incidents of violation of cybersecurity systems: Provided that information obtained by the Authority in accordance with the provisions of this subparagraph shall concern the promotion of the objects referred to in sections 15 and 16 and the performance of the functions, powers and duties of the Authority which are set out in the provisions of section 17 and may not be used for any purpose other than the purpose for which it was requested. (2) (a) Persons who are required to submit information in accordance with the provisions of subsection (1) shall respond in a timely manner and provide the details and information requested by the Authority. (b) Each operator of essential services and/or operator of critical information infrastructure, each provider of electronic communications networks and/or services and each digital service provider shall provide the Authority with any information as specified in the provisions of subsection (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) In case a person fails to comply with the relevant request of the Authority for the provision of information in accordance with the provisions of this section, an administrative fine of up to five thousand euros (€5,000) shall be imposed. (d) The Authority shall, upon a reasoned request from the Commission, provide it with the necessary information related to the performance of its duties and the information required shall be proportionate to the purpose of carrying out those duties. (e)(i) Without prejudice to Article 346 of the Treaty on the Functioning of the EU, information that is confidential, in accordance with Union 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 the provisions of this Law and of Directive 2016/1148/EU. (f)(ii) The information exchanged shall be limited to what is relevant and proportionate to the purpose of this exchange. (iii) Such exchange of information shall safeguard the confidentiality of this information and protect the security and commercial interests of operators of essential services and digital service providers. (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 has reasonable grounds to decide otherwise. (b) The Authority shall not disclose information that is covered by an obligation of professional secrecy and in particular information concerning operators of critical information infrastructure, operators of essential services and digital service providers and/or providers of electronic communications networks and services, 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: Provided that, 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: (a)Supervise the compliance with the obligations imposed by the provisions of this Law and/or the provisions of the Decisions made under the provisions of this Law, on operators of essential services, operators of critical information infrastructure, digital service providers and providers of electronic communications networks and/or services, (b)require from any operator of essential services, operator of critical information infrastructure, digital service provider or a provider of electronic communications networks and/or services 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: Provided that the installation of sensors by the Authority in internal networks can only be done at the request or consent of the operator or provider,

	(c) determine, by Decision, digital security 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; (e) impose administrative fines on operators of essential services or critical information infrastructure, or on digital service providers or providers of electronic communications networks and/or services for the violation of the provisions of this Law or of the Decisions made thereunder; (f) summon and compel, in the manner laid down in a Decision, the presence of witnesses in investigations. (2) The Commissioner shall authorize 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 electronic communications networks and systems, the provision / management of critical information infrastructure / essential information services or digital services, 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 by an employee or other representative, obstructs or prevents an employee of the Authority from performing any of his duties in accordance with the provisions of subsection (2), shall be guilty of an offence and shall, in case of conviction, be liable to imprisonment for a term not exceeding six (6) months or to a fine not exceeding eight thousand euros (€8,000) and/or to both such penalties.
Adoption of decisions.	**21**.-(1) Prior to the adoption of a Decision under the provisions of paragraph (d) of subsection (1) of section 20, any person who in the opinion of the Authority is affected or may be affected by the Decision shall be notified and shall be given the opportunity to be heard within ten (10) working days from being notified of the issuance of a Decision: Provided that the Authority shall not be obliged to give notice prior to the issuance of a Decision in case of urgency at the absolute discretion of the Authority, but in such cases the Authority shall invite the affected person to express views, within ten (10) working days from the issuance of the Decision, as to why the Decision should be revoked or amended.

	(2)After a hearing, in accordance with the provisions of subsection (1), the Commissioner shall issue and notify his final Decision to any interested party as soon as possible.
Criminal offence.	**22**. Any person who, without reasonable cause, fails to comply with the provisions of section 21 shall commit a criminal offence and, in case of conviction, shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding five thousand euros (€5,000) and/or to both such penalties.
Carrying out of an investigation.	**23.**-(1) The Authority may, ex officio, carry out an investigation into the activities and operations of any operator of essential services/critical information infrastructure, a digital service provider and a provider of electronic communications networks and/or services which are deemed to be inconsistent with the provisions and with the application of this Law and consequently make recommendations and issue Decisions as in its opinion, is appropriate. (2)For the purposes of carrying out an investigation in accordance with subsection (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/her without reasonable cause: Provided that in any case, no one is obliged to answer, if the answer may incriminate him in relation to a criminal offense or if it constitutes a breach of secrecy of communication between a lawyer-client and/or hinders or interrupts the proceedings before the Authority. (4)Any person who is convicted for the commission of a criminal offence in contravention of the provisions of paragraphs (a) and/or (b) of subsection (3) shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding five thousand euros (€5,000) and/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.	**24**.-(a) The Authority may carry out consultations with representatives of the Republic, with operators of essential services, with digital service providers, with operators of critical infrastructure or with providers of electronic communications networks and/or services and with any other persons or organizations, 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.	**26.**-(a) The Authority may, by virtue of its powers and in particular upon request by an interested operator/provider 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.
	PART SEVEN IDENTIFICATION OF OPERATORS OF ESSENTIAL SERVICES AND SIGNIFICANT DISRUPTIVE EFFECT
Identification of operators of essential services.	**27**.-(1) The Authority shall identify, for each sector and subsector referred to in a Decision issued by it, the operators of essential services and/or the operators of critical information infrastructure established in the Republic.

	(2)The criteria for the identification of the operators of essential services and/or the operators of critical information infrastructure shall be as follows: (a) the entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effect on the provision of that service. (3)For the purposes of the provisions of subsection (1), the Authority shall establish a list of the services referred to in the provisions of subsection (2). (4)For the purposes of the provisions of subsection (1), where an entity provides a service as referred to in the provisions of subsection (2), in two or more member states, the Authority shall engage in consultation with the competent authorities of other member states and that consultation shall take place before a decision on identification is taken. (5)The Authority shall, on a regular basis, and at least every two years, review and, where necessary, update the list of identified operators of essential services and/or update the relevant list of identified operators of critical information infrastructure. (6)The Authority shall participate in the cooperation group provided in section 33, which shall support member states in taking a consistent approach in the process of identification of operators of essential services. (7)For the purposes of the review by the Commission as provided in Article 23 of Directive 2016/1148/EU every two years, the Authority shall submit to the Commission the information necessary to enable the Commission to assess the implementation of Directive 2016/1148/EU, in particular the consistency of the Republic's approaches to the identification of operators of essential services.
	(8)That information shall include at least the following: (a)National measures allowing for the identification of operators of essential services; (b)the list of services referred to in the provisions of subsection (3);

	(c)the number of operators of essential services identified for each sector included in a Decision to be adopted by the Authority and an indication of their importance in relation to that sector; (d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service, as referred to in paragraph (a) of subsection (1) of section 28, or to the importance of that particular operator of essential services as referred to in paragraph (f) of subsection (1) of section 28: Provided that the Authority shall take into account any appropriate technical guidelines on parameters for the information referred to in the provisions of this subsection which are adopted by the Commission. (9)Any designation of the Central Bank as an operator of critical infrastructure or otherwise on the basis of the provisions of this Law may also be governed by an agreement concluded between the Authority and the Central Bank, which will specify the manner of application of the provisions activated by this designation, in compliance with the principle of independence of the Central Bank and of the other central banks of the European System of Central Banks, as provided by Article 130 TFEU and without prejudice to the functions, duties and powers of the Central Bank: Provided that, the powers conferred on the Authority shall be exercised in compliance with the requirements related to the security of network and information systems and the notification of incidents as these are laid down in any provision of any other legal acts which are adopted by the European Union: Provided further that, the exchange of information between the Central Bank and the Authority, within the framework of cooperation between them under the provisions of this subsection or under the provisions of section 17 and in compliance with Union law, shall not constitute a breach of the duty of confidentiality of the Central Bank or of the Authority. (10) The results of the assessment of the criticality of operators of essential services and/or operators of critical information infrastructure which is carried out by the Authority for the purposes of carrying out the provisions of this section, shall be approved by a Decision of the Council of Ministers which is classified as confidential and is not published in the Official Gazette of the Republic.
Significant disruptive effect.	**28.**-(1) When determining the significance of a disruptive effect to the provision of a service as referred to in the provisions of paragraph (c) of subsection (2) of section 27, the Authority shall take into account at least the following cross-sectoral factors:

	(a) the number of users relying on the service provided by the entity concerned; (b) the dependency of other sectors referred to in a Decision adopted by the Authority on the service provided by that entity; (c) the impact that the incidents could have, in terms of degree and duration, on economic and societal activities or public safety; (d) the market share of that entity; (e) the geographic spread with regard to the area that could be affected by an incident; (f) the importance of the operator for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service. (2) In order to determine whether an incident would have a significant disruptive effect, the Authority shall also, where appropriate, take into account sector-specific factors.
	PART EIGHT FRAMEWORK ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS
National strategy on the security of network and information systems and cybersecurity.	**29**.-(1) The Authority shall adopt a national strategy on the security of network and information systems and cybersecurity, setting out the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors and the services referred to in a Decision to be issued by the Authority. (2)The national strategy on the security of network and information systems and on cybersecurity shall be subject to consultation with interested persons prior to its adoption by the Council of Ministers and shall cover, in particular, the following issues: (a) its objectives and priorities; (b) the governance framework to achieve its objectives and priorities, including the roles and responsibilities of public authorities and other relevant bodies; (c) the identification of measures related to preparedness, response and recovery, including cooperation between the public and private sectors; (d) relevant education, awareness-raising and training programmes;

	(e) the relevant research and development plans; (f) the risk assessment plan to identify risks; (g) the list of various actors involved in its implementation; and (h) the cultivation of awareness and a culture on security. (3)The Authority may request the assistance of ENISA in developing the national strategy on the security of network and information systems. (4)The Authority shall notify its national strategy on the security of network and information systems to the Commission within three (3) months from its adoption and may exclude from such notification elements of the strategy which relate to national security.
National competent authority and single point of contact. 17(I) of 2018.	**30**.-(1) The Authority which was designated as the competent national authority on the security of network and information systems in accordance with the provisions of the Security of Networks and Information Systems Law , 2018, shall continue to be the competent authority on the security of network and information systems and as the competent authority it shall cover at least the sectors referred to in a Decision and the types of digital services referred to in a Decision issued by the Authority. (2)The Authority which was designated as the competent national authority for coordinating the implementation of the cybersecurity strategy in accordance with the provisions of the Security of Networks and Information Systems Law , 2018, and as the competent authority for coordinating the implementation of the cybersecurity strategy, shall continue to be the national authority for coordinating the implementation of the cybersecurity strategy and the competent authority for coordinating the implementation of the cybersecurity strategy. (3)The Authority shall monitor the application of the provisions of this Law in the Republic. (4)The Authority shall be designated as the national single point of contact on the security of network and information systems ('single point of contact'). (5)The Authority, as a single point of contact, shall exercise a liaison function to ensure cross-border cooperation between the Republic and the competent authorities of other member states, the Cooperation Group and the CSIRTs network referred to in section 33.

	(6)The Commissioner and the Authority shall ensure that the Authority, as the competent authority and the single point of contact, has adequate resources to carry out, in an effective and efficient manner, the tasks assigned to it and thereby to fulfil the objectives of this Law and shall ensure the effective, efficient and secure cooperation of its designated representatives in the Cooperation Group. (7)Whenever appropriate and in accordance with the relevant legislation, the Authority, as a competent authority and as the single point of contact, shall consult and cooperate with the competent national law enforcement authorities and the Commissioner for the Protection of Personal Data.
Computer security incident response team (national CSIRT).	**31**.-(1) The national CSIRT, covering at least the sectors referred to in a Decision issued by the Authority and the types of digital services referred to in a Decision to be issued by the Authority, shall be responsible for risk and incident handling in accordance with a well-defined process. (2)The national CSIRT shall meet the following requirements: (a)It shall ensure a high level of availability of its communications services by avoiding single points of failure and shall have several means available for incoming and outgoing communication with third parties at all times; the communication channels shall be clearly specified and are well known to the members of the area of responsibility and the cooperating partners, as may be defined in a Decision of the Authority, (b)It shall establish premises and supporting information systems located in secure sites; (c)It ensures business continuity: (i)the national CSIRT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate the handover of duties; (ii) the national CSIRT shall be adequately staffed to ensure a availability at all times; (iii)the national CSIRT shall rely on an infrastructure, the continuity of which is ensured and redundant systems and back-up working spaces shall be available for this purpose; (iv)it shall have the possibility to participate, if it wishes to do so, in international cooperation networks.

	(3)The Authority shall ensure that the national CSIRT has adequate resources to effectively carry out the following tasks, including at least the following: (a)monitoring of incidents at national level; (b)providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents; (c)intervention in the event of an incident; (d)providing dynamic risk and incident analysis and situational awareness; (e) participation in the CSIRTs network. (4)The national CSIRT shall establish cooperation relationships with the private sector. (5)In order to facilitate cooperation, the national CSIRT shall promote the adoption and use of common or standardised practices for: (a) incident and risk-handling procedures; (b) incident, risk and information classification schemes. (6)The Authority shall ensure effective, efficient and secure cooperation of the national CSIRT in the CSIRTs network referred to in the provisions of section 33. (7)The Authority shall ensure that the national CSIRT has access to an appropriate, secure and resilient communication and information infrastructure at national level. (8)The Authority shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of the national CSIRT. (9)The Authority may request the assistance of ENISA in developing the national and sectoral CSIRT.
International cooperation.	**32**.-(1) The Authority, as the competent authority and as the single point of contact, the national CSIRT and the sectoral CSIRT shall cooperate with regard to the fulfilment of the obligations laid down in this Law. (2)The Authority shall receive the incident notifications submitted pursuant to the provisions of this Law and the national CSIRT shall, to the extent necessary to fulfil its tasks, be granted access to data on incidents notified by operators of essential services and/or operators of critical information infrastructure, in accordance with the provisions

	of subsections (3) and (5) of section 35, or by digital service providers, in accordance with the provisions of subsections (3) and (6) of section 37. (3)The Authority shall, for the fulfilment of its duties as a single point of contact, be kept informed about notifications and the management of incidents submitted in accordance with the provisions of this Law. (4)The Authority, as a single point of contact, shall submit annually to the Cooperation Group, a summary report on the notifications received, including the number of notifications and the nature of the notified incidents, as well as the actions taken in accordance with the provisions of subsections (3) and (5) of section 35 and subsections (3) and (6) of section 37, on a date to be determined by the Cooperation Group and/or the European Commission.
	PART NINE COOPERATION
Cooperation Group and CSIRTs network.	**33**.-(1) Representatives of the Authority shall participate in the Cooperation Group established and operating in accordance with Article 11 of Directive 2016/1148/EU and shall contribute to the performance of its duties. (2)Representatives of the Authority and/or of the national CSIRT shall participate in the network of national CSIRTs established and operating in accordance with Article 12 of Directive 2016/1148/EU and shall contribute to the performance of its duties. (3)Representatives of the Authority and/or the national CSIRT shall cooperate with bodies at European level and shall represent the Republic in matters falling within its competence.
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, subject to what is otherwise provided by international agreements.

	PART TEN SECURITY OF NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES AND/OR OPERATORS OF CRITICAL INFORMATION INFRASTRUCTURE
Security requirements.	**35.**-(1)(a) Operators of essential services and/or operators of critical information infrastructure shall take appropriate and proportionate technical and organisational measures to manage the risks to the security of network and information systems which they use in their operations as such measures may be set out in a Decision issued by the Commissioner. (b) Having regard to recent state of the art, those measures shall ensure a level of security of network and information systems proportionate to the respective risk posed. (2) Operators of essential services and/or operators of critical information infrastructure shall take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the reintroduction and continuity of those services, as such measures may be set out in a Decision issued by the Commissioner. (3) (a) Operators of essential services and/or operators of critical information infrastructure shall notify the Authority without undue delay of incidents having a significant impact on the continuity of the essential services that they offer. (b) Notifications shall include information enabling the Authority and/or the national CSIRT to determine any cross-border impact of the incident. (c) Notification shall not make the notifying party subject to increased liability and the procedures and content of the notification, as well as any relevant elements shall be regulated by a Decision issued by the Commissioner. (4)In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account: (a) The number of users affected by the disruption of the essential service; (b) the duration of the incident; (c)the geographical spread with regard to the area affected by the incident.

	(5) On the basis of the information provided in the notification by the operator of essential services, the Authority or the national CSIRT shall inform the other affected member state if the incident has a significant impact on the continuity of essential services in that member state and, as part of that information, the Authority or the national CSIRT shall, in accordance with Union law or national law transposing Union law, preserve the security and commercial interests of the operator of essential services and/or the operator of critical information infrastructure, as well as the confidentiality of the information provided in its notification. (6)Where the circumstances allow, the Authority or the national CSIRT shall provide the notifying operator of essential services and/or critical information infrastructures with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling. (7)The Authority, as a single point of contact, may, in particular if there is a request from the national CSIRT, forward notifications as referred to in the provisions of subsection (5) to single points of contact of other affected Member States. (8)After consulting the notifying operator of essential services and/or operator of critical information infrastructure, the Authority or the national CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident. (9)The Authority, acting jointly with competent authorities of other Member States within the Cooperation Group, may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in the provisions of subsection (4).
Implementation and enforcement on operators of essential services and/or operators of critical information infrastructures.	**36**.-(1) The Authority shall use the necessary means to assess the compliance of operators of essential services and/or operators of critical information infrastructure with their obligations under the provisions of section 35 and the effects thereof on the security of network and information systems. (2)The Commissioner may issue a Decision on the manner of assessing the compliance of operators of essential services and/or operators of critical information infrastructure with their obligations. (3)The Authority shall use the necessary means to require operators of essential services and/or operators of critical information infrastructure to provide:

	(a)the information necessary to assess the security of their network and information systems, including documented security policies; (b)evidence of the effective implementation of security policies, such as the results of a security audit carried out by the Authority or a qualified auditor, as such authorisation may be specified in a Decision, and in the latter case, to make the results thereof, including the underlying evidence, available to the Authority. (4)The costs of security audit shall be borne by operators of essential services and/or operators of critical information infrastructure. (5)When requesting such information or evidence, the Authority shall state the purpose of the request and specify what information is required. (6)Following the assessment of the information or results of security audits referred to in subsection (3), the Authority may issue binding instructions to operators of essential services and/or operators of critical information infrastructure to remedy the deficiencies identified. (7)In dealing with incidents leading to personal data breaches, the Authority shall work in close cooperation with the Commissioner for the Protection of Personal Data.
	PART ELEVEN SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS
Security requirements.	**37**.-(1) Subject to the provisions of sections 38 and 39, digital service providers of the types set out in a Decision to be issued by the Authority shall identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems which they use in the context of offering services within the European Union. (2)These measures may be set out in a Decision issued by the Commissioner. (3)Having regard to the recent state of the art, these measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following: (a)the security of systems and facilities; (b)incident handling; (c)business continuity management; (d)monitoring, auditing and testing and exercises;

	(e)compliance with international standards. (4)Digital service providers are required to take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in a Decision to be issued by the Authority that are offered within the European Union, with a view to ensuring their reinstatement and continuity, as such measures may be set out in a Decision issued by the Commissioner. (5) (a) Subject to sections 38 and 39, digital service providers the types of which are to be mentioned in a Decision to be issued by the Authority shall notify the Authority without undue delay of any incident having a significant impact on the provision of a service that they offer within the European Union. (b) Notifications shall include information to enable the Authority and/or the national CSIRT to determine the significance of any cross-border impact. (c) Notification shall not make the notifying party subject to increased liability and the procedures and content of the notification, as well as any relevant elements shall be regulated by a Decision issued by the Commissioner. (6) In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account: (a)the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (b)the duration of the incident; (c)the geographical spread with regard to the area affected by the incident; (d)the extent of the disruption of the functioning of the service; (e)the extent of the impact on economic and societal activities. (7)The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in subsection (6). (8) Where an operator of essential services and/or an operator of critical information infrastructure relies on a third-party digital service provider for the provision of a service which is essential for the

	maintenance of critical economic and societal activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator of essential services and/or critical information infrastructure. (9) (a) Where appropriate, and in particular if the incident referred to in the provisions of subsection (5) concerns two or more member states, the Authority and/or the national CSIRT shall inform the other member states affected by the incident. (b) As part of such information, the Authority, as the competent authority and as the single point of contact, and the national CSIRT, in accordance with Union law or national law transposing Union law, shall preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided. (10) After consulting with the digital service provider concerned, the Authority or the national CSIRT and, where appropriate, the authorities or CSIRTs of other member states concerned may inform the public about individual incidents or require the digital service provider to do so, when public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest. (11) The Authority shall take into account and apply Commission implementing acts in order to specify further the elements referred to in subsection (3) and the parameters referred to in the provisions of subsection (5) of this section. (12) The Authority shall take into account and apply any Commission implementing acts laying down the formats and procedures applicable to notification requirements. (13) Subject to the provisions of subsection (2) of section 2, no further security or notification requirements shall be imposed on digital service providers. (14) (a) Digital service providers of the type referred to in a Decision to be issued by the Authority who have their establishment in the Republic or have, as defined in the provisions of section 39, a representative in the Republic, must be registered in a register that is kept by the Authority. (b) The Authority shall establish by Decision a procedure by which the digital service providers referred to in the provisions of paragraph (a) may be registered in the register. (c) A digital service provider who is not registered in the register of digital service providers maintained by the Authority as provided in the provisions of paragraph (a), shall commit a criminal offence and, in

	case of conviction, shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding five thousand euros (€5,000) or to both of these penalties.
Official Journal of the EU: L 124, 20.5.2003, p. 36	(15) The provisions of sections 37 to 39 shall not apply to micro and small enterprises as defined in the Commission's Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.
Implementation and enforcement on digital service providers.	**38.**-(1) Subject to the provisions of section 39, the Authority shall ensure that action is taken, if necessary, through ex-post supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in section 37 and such evidence may be submitted by a competent authority of another Member State where the service is provided. (2)For the application of the provisions of subsection (1), the Authority shall have the necessary powers and means to require digital service providers to: (a)provide the information necessary to assess the security of their network and information systems, including documented security policies; (b)remedy any failure to meet the requirements laid down in section 37. (3) If a digital service provider has its main establishment or a representative in the Republic, but its network and information systems are located in one or more other member states, the Authority and the competent authorities of those other member states shall cooperate and provide mutual assistance as necessary, in accordance with the provisions of Directive 2016/1148/EU. (4) If a digital service provider has its main establishment or a representative in a member state, but its network and information systems are located in the Republic or in other member states, the competent authority of the member state of the main establishment or of the representative and the Authority and/or the competent authorities of the other member states shall cooperate and assist each other, as necessary, in accordance with the provisions of Directive 2016/1148/EU. (5) Assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in the provisions of subsection (2).

Jurisdiction and territoriality.	**39**.-(1)(a) For the purposes of application of the provisions of this Law, a digital service provider shall be deemed to be under the jurisdiction of the Republic in which it has its main establishment. (b) A digital service provider shall be deemed to have its main establishment in the Republic when it has its head office in the Republic. (2) (a) A digital service provider that is not established in the European Union, but offers digital services, in accordance with the provisions of this Law and Directive 2016/1148/EU, within the European Union, shall designate a representative in the European Union. (b) In the event that paragraph (a) applies, the representative shall be deemed to be established in the Republic if he has his registered office therein. (c) The digital service provider shall be deemed to be under the jurisdiction of the Republic if the representative is established therein. (3) The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.
	PART TWELVE SECURITY OF ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES
Security and integrity of networks and services.	**40**.-(1)(a) Providers of electronic communications networks and/or services shall be required to take appropriate and proportionate technical and organisational measures to appropriately manage the risk posed to the security of electronic communications networks and services. (b) Having regard to the most advanced technical possibilities, those measures shall ensure a level of security of network and information systems proportionate to the respective risk posed. (c) In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of incidents that jeopardise the security of users and other electronic communications networks and services. (2)The Authority shall ensure that providers of electronic communications networks and/or services notify the Authority without undue delay of any security incident having a substantial impact on the operation of electronic communications networks or services.

	(3)In order to determine the significance of the impact of a security incident, the following parameters shall in particular be taken into account, where available: (a)the number of users affected by the security incident; (b)the duration of the security incident; (c)the geographical spread with regard to the area affected by the security incident; (d) the extent to which the operation of the network or service is affected to the extent of the impact on economic and social activities. (4) (a) Where appropriate, the Authority shall inform the national competent authorities in the other **m**ember **s**tates as well as ENISA. (b) The Authority may inform the public or require providers to provide such information if it considers that disclosure of the security incident is in the public interest. (c) The Authority shall submit every year to the Commission and to ENISA a summary report on the notifications received and the action taken pursuant to this subparagraph. (d) The procedures and content of the notification, as well as any relevant elements shall be regulated by a Decision issued by the Authority. (5)The Authority shall ensure that, where there is a specific and significant threat concerning an incident regarding security in electronic communications networks or services, the providers of such electronic communications networks or services inform their users who could be affected by such a threat concerning any possible protective or corrective measures that may be taken by users and, where appropriate, providers shall inform their users of the threat itself and of all possible means for preventing it, including the relevant cost: Provided that, in the event that there is a risk of a breach of the security of the network, providers of publicly available electronic communications services shall inform their contributors of such risk and of all possible means to prevent it, including the relevant cost. (6)The provisions of this section shall be without prejudice to Regulation (EU) No. 2016/679 and the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data Law. (7)For the application of the provisions of subsections (1) to (6), the Authority may impose additional requirements, in addition to any

	technical implementing measures taken by the Commission, in order to achieve the objectives of this section. (8)In order to ensure the application of the provisions of subsections (1) to (7), the Authority shall have the power to issue binding instructions on providers of electronic communications networks and/or services, including those concerning the measures necessary to respond to a security incident or to prevent such an incident, where a significant threat has been identified, and the deadlines for implementation. (9)The Authority shall have the power to require providers of electronic communications networks and/or services: (a)to provide information necessary to assess the security of their networks and services, including documented security policies, and (b)to undergo a security audit that will be carried out either by the Authority or by a qualified independent body authorised by it and make the relevant findings available to the Authority and the cost of the audit shall be borne by the provider. (10) The Authority shall have all necessary powers to investigate cases of non-compliance and their impact on the security of electronic communications networks and services on the basis of a procedure which may be determined by a Decision of the Authority. (11) In case it is established that there is a risk of a breach of the security of the electronic communications network due to the use of the service, the Authority may request providers of electronic communications services to take measures, including temporary measures, such as the interruption of the service. (12) For the application of the provisions of subsections (1) to (7), the Authority shall have the power to make use of services from the national CSIRT, which forms part of the Authority. (13) Where appropriate and in accordance with the relevant legislation, the Authority shall consult and cooperate with the competent national law enforcement authorities and with the Commissioner for the Protection of Personal Data.
	PART THIRTEEN STANDARDISATION AND VOLUNTARY NOTIFICATION
Standardization.	**41**.-(1) The Authority shall encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

	(2) The Authority shall cooperate with ENISA and the other member states in order to draw up advice and guidelines regarding the technical areas to be considered in relation to subsection (1), as well as regarding already existing standards, including member states' national standards covering those areas.
Voluntary notification.	**42.**-(1) Without prejudice to the provisions of paragraph (cc) of section 17, entities which have not been identified as operators of essential services and/or operators of critical information infrastructure and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide. (2)When processing notifications, the Authority shall act in accordance with the procedure set out in section 35. (3)The Authority may prioritise the processing of mandatory over voluntary notifications. (4)Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on the Authority. (5)Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject to had it not given that notification.
	PART FOURTEEN PENALTIES
Administrative fine.	**43**.-(1) In case that the Authority ascertains that a person does an act or makes an omission by infringement of the provisions of this Law, it may impose an administrative fine on such person for an amount not exceeding two hundred thousand euros (€200,000), depending on the gravity of the infringement, and, in case of repetition of the infringement, a fine not exceeding ten thousand euros (€10,000) for every day that the infringement continues: Provided that the procedure for the imposition of the administrative fine shall be prescribed by a Decision of the Authority. (2)The Authority may impose an administrative fine on any person who does an act or makes an omission, by infringement of the provisions of any Decisions and/or Regulations of the European Union not exceeding three hundred thousand four hundred euros (€300,400) and, in case of repetition of the infringement, an administrative fine not exceeding two hundred thousand euros (€200,000).

	(3)The Authority may adopt a Decision regarding the procedure for imposing a fine and/or other administrative penalties. (4)Before the Authority imposes an administrative fine, the Commissioner 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. (5)The Authority shall impose an administrative fine under the provisions of subsection (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 72(I) of 2018.	(a) on his right to challenge the decision by recourse to the Administrative Court, in accordance with the provisions of Article 146 of the Constitution and the Establishment and Operation of an Administrative Court Law,2015, and (b) the period within which the aforementioned right may be exercised.
	(6)In case of refusal or omission by a person to whom an administrative fine was imposed under the provisions of this Law to pay such fine to the Authority, the Authority shall take judicial measures and collect the sums due as a civil debt owed to the Republic.
Criminal offenses.	**44**.-(1) An operator of essential services and/or an operator of critical information infrastructure who fails to notify the Authority, without undue delay, an incident which has a serious impact on the continuity of its essential services shall be guilty of an offence and, in case of conviction, shall be liable to imprisonment for a term not exceeding two (2) years or to a fine not exceeding ten thousand euros (€10,000) or to both such penalties. (2)A digital service provider who fails to notify the Authority, without undue delay, of an incident which has a significant impact on the provision of the service it provides, shall be guilty of an offence and in case of conviction, shall be liable to imprisonment for a term not exceeding two (2) years or to a fine not exceeding ten thousand euros (€10,000) or to both such penalties. (3)An operator of essential services and/or an operator of critical information infrastructure who fails to take appropriate and proportionate technical and organisational measures to manage the risks to the security of the network and information systems that it uses during its activities, shall be guilty of an offence and shall on conviction be liable to imprisonment for a term not exceeding three (3) years or

	to a fine not exceeding fifteen thousand euros (€15,000) and/or to both such penalties. (4)A digital service provider who fails to take appropriate and proportionate technical and organisational measures to manage the risks to the security of the networks and information systems that it uses in the context of the provision of the services referred to in a Decision to be issued by the Authority, shall be guilty of an offence and shall, in case of conviction, be subject to imprisonment for a term not exceeding three (3) years or to a fine not exceeding fifteen thousand euros (€15,000) or to both such penalties. (5) Any person who does not provide any information requested by the Authority, in accordance with the provisions of paragraph (b) of subsection (1) of section 20 within fifteen (15) days from the date of the request, shall be guilty of an offence and shall, in case of conviction, be liable to imprisonment for a term not exceeding three (3) years or to a fine not exceeding three thousand four hundred euros (€3,400). (6) Any person whom the Authority requires to provide any information, in accordance with the relevant provisions of Regulations issued by the European Union, and omits to do so within the specified date of fifteen (15) days from the date of the request, shall be guilty of an offence and shall, in case of conviction, be liable to imprisonment for a term not exceeding six (6) months or to a fine not exceeding three thousand four hundred euros (€3,400) or to both such penalties. (7)Any person who contravenes any provision of the Decisions and/or Regulations of the European Union regarding the security of networks and information systems, shall be guilty of an offence and shall, in case of conviction, be liable to imprisonment for a term not exceeding three (3) years or to a fine not exceeding fifteen thousand euros (€15,000) or to both such penalties.
	PART FIFTEEN REGULATIONS, DECISIONS, FINANCIAL PROVISIONS, REPORTS AND VARIOUS OTHER MATTERS
Issuance of Regulations.	**45**.-(1) For the better carrying out of the provisions of this Law, the Council of Ministers shall make 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 subsection (1), these Regulations may provide, inter alia, for the following:

	(a)The methodology for calculating fees to finance the costs of the Authority; (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, functions and qualifications of the permanent staff of the Authority; (d)the Health Care Fund to cover the members of staff of the Authority during and after their service with the Authority in accordance with the provisions of the Regulation on Electronic Communications and Postal Regulation (Health Care Fund) Regulations and the provisions of the General Health System Law; (e)the Provident Fund for the employees of the Authority during their service with the Authority; (g)the Provident Fund for Hourly Paid Personnel for hourly paid members of staff of the Authority.
Issuance of Decisions by the Authority.	**46**.-(1) For the better out 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 subsection (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 provided by the provisions of this Law, required or needs to be prescribed.

	(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 date of entry into force, from the date of such publication of the relevant Decision: Provided that 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 Decision, the Regulations of the European Union relating to the security of networks and information systems and cybersecurity.
Budget. 20(I) of 2004 123(I) of 2016 133(I) of 2016 159(I) of 2017.	**47**.-(1) The Authority shall establish a budget of revenue and expenditures for each financial year, beginning on the 1st of January and ending on the 31st of December. (2)The budget shall be submitted by the Minister to the Council of Ministers by the 1st of July every year and shall be subject to the approval of the Council of Ministers and the House of Representatives, subject to the provisions of section 104 of the Fiscal Responsibility and Financial Framework Law. (3)Following any amendments by the Council of Ministers, the budget shall be submitted to the House of Representatives before the 30th of September every year. (4)The budget shall cover the Authority's financial programme for each financial year, which shall run from the 1st of January to the 31st of December: Provided that the first financial programme of the Authority shall start from the date of operation of the Authority and shall end on the 31st of December of the same year. (5)The manner in which the budget shall be prepared and the manner in which the funds will be displayed in the table of revenue and expenditure shall be similar to the manner in which the state budget is drawn up. (6)The Authority shall ensure the preparation of a budget referred to in the provisions of subsection (1) and the preparation of the financial plan referred to in the provisions of subsection (4). (7)In case of failure to adopt the budget in due time, the Authority shall operate in accordance with the provisions of Article 168(3) of the Constitution on the State budget relating to twelfths.

Book Keeping.	**48**.-(1) The Authority shall keep appropriate books and accounts for its activities, as determined from time to time 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 from time to time 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 submits the financial management report to the Council of Ministers and the House of Representatives for information. (5)The Authority shall ensure that the books and accounts referred to in subsection (1), (2) and (4) are kept and reports are drawn up.
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 from the date of expiry 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**. In the event that the Authority ceases to exist for any reason, the posts of the permanent staff and the holders of the posts , as well as vacant posts shall be transferred to an appropriate ministry, department or service of the government, and in the event that the functions, powers and duties of the Authority under the provisions of this Law are transferred for any reason to another legal person, authority or body, the staff of the Authority shall provide services to the said legal person, authority or body without any change in their status or in their terms of service.
Assets of the Authority, in case it ceases to exist.	**51**. If the Authority ceases to exist for any reason, all the assets of the Authority shall devolve upon the Republic.
Recourse to the Administrative Court against the 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 Establishment and Operation of an Administrative Court Law. (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 this information to the Commission or another institution of the European Union upon a reasoned request.

Liability of the Commissioner, of the Deputy Commissioner and of the members of staff of the Authority.	**53.** Subject to the provisions of this Law, and the Regulations and Decisions made 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 the *bona fide* exercise of their respective duties and their functions and powers under the provisions of this Law.
Liability of legal persons.	**54.**(1) A legal person shall be guilty of an offence provided for by sections 22 and 43 where the offence is committed for the benefit of the legal person by any person acting either individually or as part of a body of that legal person and holding a leading position in that legal person in the capacity of: (a)an authorised representative of the legal person; (b)a proxy holder authorised to take decisions on behalf of the legal person, or (c)a proxy holder authorised to exercise control within the legal person. (2)A legal person shall be guilty of an offence referred to in sections 22 and 43 where the lack of supervision or control by a person specified in the provisions of subsection (1) has enabled the commission of that offence for the benefit of the legal person by a person acting under the authority of the person specified in the provisions of subsection (1). (3)Without prejudice to the provisions of subsections (1) and (2), the liability of the legal person 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 provided by the provisions of sections 22 and 43. (4)Without prejudice to the provisions of subsections (1) and (2), a person who advises, promotes or induces another person to participate in the commission or attempt to commit an offence provided by the provisions of sections 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 he had committed such an act himself. (5)In the event that an act or omission of a legal person 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 responsibility for the act or omission for the payment of the administrative fine shall lie with the legal persons, as well as the natural persons referred to in the provisions of subsection (1).

	PART SIXTEEN TRANSITIONAL AND FINAL PROVISIONS
Transitional provision.	**55.**-(1) Decisions or Regulations made pursuant to the Security of Networks and Information Systems Law , 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 or notifications to the Commission, as the case may be, to be made under the provisions of this Law. (2) Any reference to "OCECPR" in the relevant legislation or in Regulations or Orders made 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".
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, 2018 shall be repealed.