E

9875

NEWSPAPER
THE GOVERNMENT
OF THE HELLENIC REPUBLIC

November 27, 2024 | ISSUE ONE | Sheet No. **195**

LAW NO. 5160

Incorporation of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS Directive 2) and other provisions.

THE PRESIDENT
OF THE HELLENIC REPUBLIC

We enact the following law passed by Parliament:

TABLE OF CONTENTS

PART A

INCORPORATING DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 14 DECEMBER 2022

CHAPTER A
PURPOSE AND OBJECT

Article 1
Purpose

The purpose of this Part is to achieve a high level of cybersecurity by implementing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS Directive 2, L 333).

Article 2
Subject matter (Article 1 of Directive (EU) 2022/2555)

The subject of this Part is:
a) the introduction of regulations for the National Cybersecurity Strategy, the designation of a competent authority for cybersecurity and cyber crisis management, the designation of a single point of contact for cybersecurity and response teams for incidents related to computer security [Computer Security

Incident Response Team (CSIRT)],
b) the definition of risk management measures in the field of cybersecurity and the imposition of reporting obligations for entities falling within the scope of this Part, including entities designated as critical in accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Directive 2008/114/EC

Council EC (L 333),
c) the provision of rules and obligations regarding the exchange of information on cybersecurity
and
d) the establishment of provisions for the general supervision and imposition of measures and sanctions for the implementation of this Part, so as to achieve a high level of cybersecurity in Greece within the framework of the rules and objectives of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union,

the amendment of Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and the repeal of Directive (EU) 2016/1148 (NIS Directive 2).

CHAPTER B
GENERAL PROVISIONS

Article 3
Scope
(Article 2 of Directive (EU) 2022/2555)

1. This Part shall apply to public or private entities of the types referred to in Annexes I or II to this Law, which are classified as medium-sized enterprises in accordance with paragraph 1 of Article 2 of the Annex to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (L 124), or which exceed the thresholds for medium-sized enterprises referred to in that Article and which are established or provide their services or carry out their activities within the Greek territory. Paragraph 4 of Article 3 of the Annex to the said Recommendation shall not apply for the purposes of this Part.

2. This Part also applies to entities, sectors and subsectors listed in Annexes I or II, regardless of their size, provided that:

a) the services are provided by: aa) providers of public electronic communications networks or publicly available electronic communications services, ab) trust service providers, ag) top-level domain name registries and domain name system service providers,

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

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

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

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

f) the entity is: a) a central government body , as defined in paragraph c of paragraph 1 of article 14 of Law 4270/2014 (Government Gazette 143), fb) a first-degree Local Government Organization, fc) a second-degree Local Government Organization.

3. This Part applies to entities that are classified as critical entities in accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (L 333), regardless of their size.

4. This Part applies to entities providing domain name registration services, regardless of their size.

5. This Part shall apply without prejudice to measures taken by the country to protect its national security and its sovereign right to safeguard other essential State functions, including safeguarding its territorial integrity and maintaining public order.

6. This Part shall not apply to public administration entities carrying out their activities in the fields of national security, public order, defence or law enforcement, including the prevention, detection, investigation and prosecution of criminal offences. The supervisory and enforcement measures referred to in Chapter G of this Part shall not apply to entities exempted in accordance with the first subparagraph of point (b) of paragraph 2 of Article 30.

7. Paragraph 6 and paragraph b) of paragraph 2 of article 30 shall not apply when an entity acts as a trust service provider, in accordance with paragraph 16 of article 3 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

8. This Part does not apply to entities which Greece excludes from the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 (L 333), in accordance with paragraph 4 of Article 2 of that Regulation.

9. The obligations provided for in this Part do not include the provision of information, the disclosure of which would be contrary to the essential interests of national security, public order or defence of the country.

10. This law shall apply without prejudice to 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 (General Data Protection Regulation, L 119), Law 4624/2019 (Government Gazette ÿ' 137), Law 3471/2006 (Government Gazette ÿ' 133),

Law 4267/2014 (Government Gazette 137), Law 4411/2016 (Government Gazette 142) and Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (L 333).

11. Without prejudice to Article 346 of the Treaty on the Functioning of the European Union, information which is confidential under Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other competent authorities in accordance with this Law only to the extent that such exchange is necessary for the implementation of the

implementation of its provisions. The information exchanged shall be limited to what is relevant and proportionate to the purpose of such exchange. The exchange of information shall preserve the confidentiality of such information and protect the security and commercial interests of the entities concerned.

12. The entities, the National Cybersecurity Authority of Article 3 of Law 5086/2024 (A' 23) and the CSIRTs of Article 10 hereof shall process personal data to the extent necessary for the purposes of this Law and in accordance with Regulation (EU) 2016/679, only if such processing is based on Article 6 of that Regulation. The processing of personal data under this Part by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with European Union law on data protection and the protection of privacy, as well as with Law 4624/2019 and Law 3471/2006.

Article 4
Key and important entities
(Article 3 of Directive (EU) 2022/2555)

1. For the purposes of this Part, "basic "entities" are considered to be the following entities:

a) entities in the sectors and subsectors listed in Annex I, which exceed the thresholds for medium-sized enterprises set out in paragraph 1 of Article 2 of the Annex to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.12.2003, p. 1);

b) approved trust service providers and top-level domain name registries, as well as Domain Name System service providers , regardless of their size,

c) providers of public electronic communications networks or publicly available electronic communications services that are classified as medium-sized enterprises, pursuant to paragraph 1 of Article 2 of the Annex to Recommendation 2003/361/EC,

d) entities referred to in sub-paragraph (a) of paragraph f) of paragraph 2 of article 3 of this article,

e) any other entities of the sectors and sub-sectors referred to in Annexes I or II, which are identified as key entities in accordance with paragraphs b) to e) of paragraph 2 of Article 3 hereof,

f) entities referred to in paragraph 3 of Article 3 hereof, which are identified as critical entities in accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (L 333),

g) entities recognized, in accordance with article 4 of law 4577/2018 (Government Gazette A' 199) and article 16 of decision no. 1027/4.10.2019 of the Minister of of the State (B' 3739), before January 16, 2023, as operators of essential services.

2. For the purposes of this Part, entities in the sectors and subsectors listed in Annexes I or II that are not considered to be key entities in accordance with paragraph 1 shall be considered to be significant entities. These include entities identified as significant entities in accordance with paragraphs b) to e) of paragraph 2 of Article 3.

3. The National Cybersecurity Authority, in cooperation with the competent regulatory/supervisory authorities and other national bodies involved in each sector, shall identify the key or significant entities referred to in points c) to e) of paragraph 2 of Article 3 that fall within the scope of this Regulation. The National Cybersecurity Authority shall draw up a list of key and significant entities, as well as entities that provide domain name registration services, in accordance with paragraph 3 of Article 30. In order to draw up the list, the entities referred to in it shall submit to the National Cybersecurity Authority, through the digital platform or in any other manner specified by the decision of paragraph 4 of Article 30, within a period of two (2) months from the entry into force of this Regulation, the following information:

a) the name of the entity,

b) the address and updated contact details, including email addresses and telephone numbers of the entity, the range of internet addresses (IP ranges),

c) the set of domain names used by the entity,

(d) where applicable, the relevant sector, subsector and type of entity referred to in Annexes I or II and

(e) where applicable, a list of the other Member States of the European Union in which they provide services falling within the scope of this Part.

4. The entities of par. 3 shall notify the National Cybersecurity Authority of changes to the data submitted through the digital platform of par. 4 of article 30, without delay and in any case within two (2) weeks from the date of occurrence of the change, without prejudice to par. 2 of article 19.

5. No later than April 17, 2025 and every two (2) years, the National Cybersecurity Authority shall notify:

a) to the European Commission and the Cooperation Group to support and facilitate strategic cooperation and information exchange between Member States, as well as to enhance trust and confidence , the number of key and significant entities in accordance with paragraph 3 for each sector and sub-sector referred to in Annexes I or II and

b) to the European Commission, information on the number of key and significant entities

which are identified in accordance with paragraphs b) to e) of paragraph 2 of article 3, the sector and sub-sector referred to in Annexes I or II to which they belong, the type of service they provide and the decision of paragraph 3 of article 30.

6. By 17 April 2025 and upon request of the European Commission, the National Cybersecurity Authority shall notify the European Commission of the names of the key and significant entities referred to in point b) of paragraph 5.

Article 5
Reservation regarding sectoral legal acts of the Union
(Article 4 of Directive (EU) 2022/2555)

1. Where sectoral legal acts of the European Union and their national harmonisation provisions require key or significant entities to adopt cybersecurity risk management measures or to notify significant circumstances and where those requirements are at least equivalent in effect to the obligations laid down herein, the relevant provisions of this Law, including the provisions on supervision and enforcement set out in Chapter G, shall not apply to those entities. Where sectoral legal acts of the European Union and their national harmonisation provisions do not cover all entities in a specific area falling within the scope of this Law, the provisions of this Law shall continue to apply to entities not covered by those sectoral legal acts of the European Union.

2. The requirements referred to in paragraph 1 shall be considered equivalent in effect to the obligations set out in this Part when:

a) the risk management measures in the field of cybersecurity are at least equivalent in effect to those provided for in paragraphs 1 and 2 of article 15 or

b) the sectoral legal act of the European Union provides for immediate access, where appropriate automatic and direct, to incident notifications by the CSIRT of the National Cybersecurity Authority and provided that the requirements for the notification of significant incidents are at least equivalent in effect to those set out in paragraphs 1 to 6 of Article 16.

3. The provisions of this Regulation on cybersecurity risk management and incident reporting obligations and on supervision shall not apply to financial entities covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 (L 333), in each case

case of the obligation to cooperate with the National Cybersecurity Authority, in accordance with article 13 hereof.

Article 6
Definitions
(Article 6 of Directive (EU) 2022/2555)

For the application of this law, the following definitions apply:

a) "network and information system":

aa) electronic communications network, as defined in sub-paragraph 9) of paragraph A of article 110 of the Law 4727/2020 (A' 184),

ab) any device or group of interconnected or related devices, one or more of which, in accordance with a program, carries out automatic processing of digital data or

ag) digital data stored, processed, retrieved or transmitted by elements covered by sub-paragraphs aa) and ab) hereof for the purposes of their operation, use, protection and maintenance,

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

(c) "cybersecurity" means cybersecurity as defined in point (1) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA ("European Union Agency for Cybersecurity") and on cybersecurity certification in the information and communications technology sector and repealing Regulation (EU) 526/2013 (Cybersecurity Act, L 151),

d) "National Cybersecurity Strategy": a coherent framework that provides strategic objectives and priorities in the field of cybersecurity and the governance for their achievement,

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

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

(g) “large-scale cybersecurity incident”: an incident that causes a disruption that exceeds the country’s capacity to respond to it or that has a significant impact on at least two Member States of the European Union;

(h) “incident management” means any action and process aimed at preventing, detecting, analysing and containing or responding to and recovering from an incident;

(i) "risk": the probability of loss or disruption caused by an event and expressed as a combination of the magnitude of that loss or disruption and the probability of that event occurring;

j) “cyber threat”: cyber threat, as defined in point 8) of Article 2 of Regulation (EU) 2019/881,

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

(l) “ICT product”: product, as defined in paragraph 12) of article 2 of Regulation (EU) 2019/881,

m) "ICT service": ICT service, as defined in point 13) of Article 2 of Regulation (EU) 2019/881,

n) "ICT procedure": ICT procedure, as defined in point (14) of Article 2 of Regulation (EU) 2019/881,

(o) “vulnerability” means a weakness, sensitivity or defect in ICT products or ICT services that can be exploited by a cyber threat;

p) “standard”: standard, as defined in point 1) of Article 2 of Regulation (EU) 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardization, amending Council Directives 89/686/

EEC and 93/15/EEC and Directives of the European Parliament and of the Council 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 and repealing Council Decision 87/95/ EEC and Decision 1673/2006/EC of the European Parliament and of the Council (L 316),

q) “technical specification”: technical specification, as defined in point 4) of Article 2 of Regulation (EU) 1025/2012,

(r) ‘internet exchange point’ means a network facility that allows the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides an interconnection only for autonomous systems and which neither requires internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise affects such traffic;

(s) ‘Domain Name System’ or ‘DNS’: a hierarchical distributed naming system that allows the identification of Internet services and resources, allowing end-user devices to use Internet routing and connectivity services to access those services and resources;

(k) “DNS service provider”: an entity that provides: (k) publicly available recursive domain name resolution services for end-users of the Internet or (kb) authoritative domain name resolution services for use by third parties, with the exception of root name servers,

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

(vb) ‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of a registrar, such as a provider of personal data registration services or an agent or reseller;

yc) "digital service": service, as defined in paragraph b) of paragraph 2 of article 2 of Presidential Decree 81/2018 (Government Gazette A' 151),

(k) “trust service”: technical specification, as defined in point 16) of Article 3 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 (L 257),

(k) "trust service provider": trust service provider, as defined in point (19) of Article 3 of Regulation (EU) 910/2014,

(xf) “qualified trust service”: qualified trust service, as defined in point (17) of Article 3 of Regulation (EU) 910/2014,

(g) "qualified trust service provider": qualified trust service provider, as defined in point (20) of Article 3 of Regulation (EU) 910/2014,

(k) "online/internet market": online/ online market, as defined in paragraph 7 of article 3 of law 2251/1994 (Government Gazette A' 191),

(v) “online/internet search engine”: online/internet search engine, as defined in paragraph 5) of Article 2 of the Regulation

(EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fair treatment and transparency for business users of online intermediation services (L 186),

(l) “cloud computing service”: a digital service that enables on-demand management and widespread remote access to a scalable and elastic pool of shared computing resources , including when these resources are distributed across multiple locations;

(la) “data center service”: a service that includes structures, or groups of structures, intended for the central hosting, interconnection and operation of information technology and network equipment and providing data storage, processing and transmission services , as well as all power distribution and environmental control facilities and infrastructure ;

(lv) “content distribution network”: a network of geographically distributed servers aimed at ensuring high availability and accessibility or rapid delivery of digital content and digital services to internet users on behalf of content and service providers;

(lg) ‘social networking service platform’: a platform that allows end users to connect, exchange, search and communicate with each other through multiple electronic means, in particular through conversations, posts, videos and recommendations;

ld) “representative”: a natural or legal person established in Greece who has been expressly designated to act on behalf of a Domain Name System service provider (DNS), top-level domain name registry (TLD), entity providing domain name registration services , cloud computing service provider, data center service provider, content distribution network provider, managed service provider, managed security service provider, online/internet marketplace provider , online/internet search engine or social networking service platform not established in the European Union, to which the National Cybersecurity Authority or CSIRT may address itself instead of the entity itself with regard to the obligations of that entity under this law,

(e) ‘public administration entity’ means an entity recognised as such under national law, not including courts, parliaments or the central bank, which meets the following criteria:

(ea) it has been established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character,

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

(e) is financed for the most part by the State, regional authorities or other bodies governed by public law, is subject to management control by such authorities or bodies or has an administrative, management or supervisory board, more than half of whose members are appointed by the State, regional authorities or other bodies governed by public law,

(d) has the power to issue administrative acts affecting the rights of natural or legal persons in the cross-border movement of persons, goods, services or capital,

(l) “public electronic communications network”: public electronic communications network, as defined in sub-paragraph 5) of paragraph A of article 110 of the Law 4727/2020,

lg) “electronic communications service”: electronic communications service, as defined in sub -paragraph 39) of paragraph A of article 110 of Law 4727/2020,

(l) ‘entity’ means a natural or legal person established and recognised as such under the national law of its place of establishment or of the place of provision of services and pursuit of activities, which may, acting on its own behalf, exercise rights and be subject to obligations;

(lh) ‘managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of information and communication technology (ICT) products, networks, infrastructure, applications or any other network and information systems, through assistance or active management performed either at the customer’s premises or remotely ;

(m) “managed security service provider”: a managed service provider that performs or provides support for activities related to cybersecurity risk management, including incident response, penetration testing and security audits;

(ma) “research organization”: an entity whose primary objective is to conduct applied research or experimental development with a view to exploiting the results of such research for commercial purposes, but does not include educational institutions.

CHAPTER C
COORDINATED REGULATIONS CYBERSECURITY FRAMEWORK

Article 7
National Cybersecurity Strategy (Article 7 of Directive (EU) 2022/2555)

1. The National Cybersecurity Authority formulates the National Cybersecurity Strategy (NCS) which provides for the strategic objectives, the resources required to achieve these objectives and appropriate policy and regulatory measures, with the aim of achieving and maintaining a high level of

cybersecurity. The E.S.K. is established within the framework of the National Security Strategy formulated by the Government National Security Council, in accordance with par. 5 of article 7 of law 4622/2019 (A' 133).

The E.S.K. includes in particular:

(a) objectives and priorities of the cybersecurity strategy , covering in particular the areas referred to in Annexes I and II;

b) governance framework for the achievement of the objectives and priorities referred to in paragraph a), including the policies referred to in paragraph 2,

(c) a governance framework clarifying the roles and responsibilities of the relevant stakeholders at national level, which supports cooperation and coordination at national level between competent authorities, the single point of contact and CSIRTs, pursuant to this Part, as well as coordination and cooperation between those bodies and competent authorities under sectoral legal acts of the European Union;

d) mechanism for determining the relevant data and risk assessment,

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

f) list of authorities and stakeholders who participate in the implementation of the E.S.K.,

(g) a policy framework for enhanced coordination between competent authorities under this Part and the competent authorities provided for in Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (L 333) on the exchange of information on risks, cyber threats and incidents, as well as on risks, threats and incidents outside cyberspace, and the exercise of supervisory tasks, where appropriate;

h) a plan, including the necessary measures , to enhance the general level of awareness of citizens in the field of cybersecurity,

i) the critical success factors for achieving implementation of strategic and operational objectives.

2. Within the framework of the E.S.K., policies are established in particular:

a) embedding cybersecurity in the supply chain of information and communication technology (ICT) products and ICT services used by entities to provide their services,

(b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including those relating to cybersecurity certification, encryption , in cooperation with the competent national authority;

CRYPTO, and the use of open source cybersecurity products,

c) vulnerability management, including the promotion and facilitation of coordinated vulnerability disclosure in accordance with paragraph 1 of Article 12,

(d) relating to maintaining the general availability , integrity and confidentiality of the public core of the open Internet, including, where applicable, the cybersecurity of submarine communications cables;

e) promoting the development and integration of advanced technologies with the aim of implementing advanced risk management measures in the field of cybersecurity,

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

g) support for academic and research institutions to develop, strengthen and promote the development of cybersecurity tools and secure network infrastructures,

h) including relevant procedures and appropriate information exchange tools to support the voluntary exchange of cybersecurity information between entities in accordance with European Union law and this law,

(i) strengthening the cyber resilience and cyber health of small and medium-sized enterprises, in particular those excluded from the scope of this Part, by providing easily accessible guidance and assistance for their specific needs;

j) promoting active cyber protection.

3. The National Cybersecurity Authority shall notify the NCA to the European Commission within three (3) months of its approval in accordance with the first paragraph of paragraph 5 of article 30. Information relating to national security shall be excluded from the above notification.

4. The E.S.K. is evaluated on a regular basis and at least every five (5) years based on key performance indicators and, where necessary, is updated in accordance with the second paragraph of par. 5 of article 30. The Action Plan for the implementation of the E.S.K. is evaluated and, if necessary, updated at least every two (2) years in accordance with the second paragraph of par. 5 of article 30.

5. The National Cybersecurity Authority may submit, if it deems it necessary, a request to the European Union Agency for Cybersecurity (ENISA) for its assistance in the development or updating of the National Cybersecurity Strategy and the key performance indicators for its evaluation, with a view to its harmonization with this law.

Article 8
Competent authority and single point of contact
(Article 8 of Directive (EU) 2022/2555)

1. The National Cybersecurity Authority is designated as the competent authority responsible for cybersecurity and for the supervisory tasks referred to in Chapter G of this Part and participates in the Cooperation Group to support and facilitate strategic cooperation and the exchange of information between Member States, as well as to strengthen trust and confidence, in accordance with Article 14 of Directive 2022/2555.

2. The National Cybersecurity Authority shall monitor the implementation of this Part and shall be the single point of contact for Greece. Within the framework of its responsibilities, the National Cybersecurity Authority shall act as a liaison to ensure cross- border cooperation of the country with the competent authorities of other Member States and, where appropriate, with the European Commission and the European Union Agency for Cybersecurity (ENISA), as well as to ensure cross-sectoral cooperation with other competent authorities within the country.

3. The National Cybersecurity Authority shall notify the European Commission, without delay, of its designation as competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 2, its tasks, as well as any subsequent changes. The National Cybersecurity Authority shall publish its designation as competent authority on its website.

Article 9
National cyber crisis management framework
(Article 9 of Directive (EU) 2022/2555)

1. The National Cybersecurity Authority is designated as responsible for the management of large-scale incidents and crises in the field of cybersecurity (cyber crisis management authority) and participates in the European Network of Liaison Organizations for Cyber Crises (EU-CyCLONe).

2. In order to define the objectives and the procedure for the management of large-scale incidents and crises in the field of cybersecurity, a national plan for responding to large- scale incidents and crises in cyberspace shall be drawn up in accordance with paragraph 7 of article 30. This plan shall specify in particular:

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

b) the duties and responsibilities of the National Cybersecurity Authority as a cyber crisis management authority,

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

d) national preparedness measures, including of exercises and training activities,

e) public and private stakeholders sector and infrastructure, and

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

The decision of par. 7 of article 30, by which the national plan for dealing with large-scale incidents and crises in cyberspace is drawn up , is approved within an exclusive period of one (1) month from its submission to the Coordination Committee for Cybersecurity issues of article 23 of law 5002/2022 (A' 228), and in the event of inaction within the above deadline, it is presumed to have been tacitly approved. The legal effects of the decision of the Governor of the National Cybersecurity Authority occur either from the day following its explicit approval or from the day following the lapse of one (1) month from its submission to the Committee. The national emergency plan of par. c) of article 22 of

Law 5002/2022 is part of the national plan hereof.

3. The National Cybersecurity Authority shall notify the European Commission, within three (3) months from the entry into force of this Regulation, of its designation as the competent authority referred to in paragraph 1 and shall inform it, without delay, of any subsequent changes. In addition, the National Cybersecurity Authority shall submit to the European Commission and to the European Network of Cyber Crisis Liaison Organizations (EU-CyCLONe), within three (3) months from the approval of the national plan for responding to large-scale incidents and crises in the field of cybersecurity, information on the requirements of paragraph 2 with regard to the national plan. Specific information shall be exempted from the provision of information , if deemed necessary for reasons of national security.

Article 10
Response teams for incidents involving in computer security (CSIRTs)
(Article 10 of Directive (EU) 2022/2555)

1. The National Cybersecurity Authority is designated as the competent Computer Security Incident Response Team (CSIRT) for the entities falling within the scope of this part . Specifically for the organizations referred to in point f) of paragraph 2 of article 3, the competent Computer Security Incident Response Team (CSIRT) is the Cybersecurity Response Team (National CERT) of the Cyberspace Directorate of the National Intelligence Service (NIS).

2. If deemed necessary to achieve a high level of cybersecurity, other CSIRTs may be designated , in accordance with paragraph 8 of article 30.

3. The CSIRT of the National Cybersecurity Authority shall perform a coordinating role for CSIRTs, in order to achieve the objectives of this article. The CSIRTs shall comply with

are in compliance with the requirements set out in paragraph 1 of Article 11, cover at least the sectors and sub-sectors referred to in Annexes I and II and are responsible for handling incidents. CSIRTs shall handle incidents concerning computer security in the relevant sector, if their assistance is requested by the National Cybersecurity Authority, in particular in cases of serious, urgent or significant number of incidents developing simultaneously. For incidents concerning the entities referred to in paragraph f) of paragraph 2 of article 3, is handled directly by the Cybersecurity Response Team (National CERT) of the Cyberspace Directorate of the Hellenic Republic. The CSIRTs are obliged to promptly inform the National Cybersecurity Authority of incidents they detect that concern cybersecurity , as well as to promptly assist it in carrying out its duties in accordance with par. 1, if requested by the same.

4. CSIRTs shall exchange information with key and significant entities and other relevant stakeholders , through secure information exchange tools . The CSIRT of the National Cybersecurity Authority and other CSIRTs shall cooperate and, where appropriate, exchange information through the National Cybersecurity Authority in accordance with Article 21 hereof with sectoral or cross-sectoral communities of key and significant entities. In addition, they participate in peer reviews organised in accordance with Article 19 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (L 333) and seek their effective, efficient and secure cooperation within the framework of the CSIRTs network.

5. CSIRTs may establish cooperative relations with national computer security incident response teams of a third country, in particular by exchanging information, using relevant information exchange protocols, including the traffic light protocol (TLP), and may exchange relevant information with them, including personal data in accordance with 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 (General Data Protection Regulation, L 119). In addition, they may cooperate with national computer incident response teams of a third country or with equivalent third country bodies, in particular with a view to providing assistance in the field of cybersecurity .

6. In order to deal with incidents in the field of cybersecurity, special response teams may be established , in accordance with paragraph 9 of article 30. These response teams shall consist of representatives of the National Cybersecurity Authority, and representatives of either the competent organizational unit of the General Staff of National Defence for cyber defence issues, or of the Cyberspace Directorate of the National Intelligence Service or, where applicable, of the National Sectorial Focal Points (NSFP) of paragraph 6 of article 13. The duties of Coordinator shall be assigned to a representative of the National Cybersecurity Authority. The representatives of the other services shall be designated by the competent bodies, as the case may be, upon request of the Commander of the National Cybersecurity Authority. In the event of failure to appoint a representative within the deadline set by the Director of the National Cybersecurity Authority, the Director's decision to establish the response team shall be issued without the participation of a representative of the relevant service. For each incident, each special response team shall submit to the competent organizational unit of the National Cybersecurity Authority a preliminary report within twenty -four (24) hours, a more complete updated report within seventy-two (72) hours, or whenever requested by the competent organizational unit of the National Cybersecurity Authority, as well as a detailed report on the incident and its management, within one (1) month from the issuance of the decision to establish the team. The expenses of the team members for the execution of the task assigned to them shall be borne by the budget of the National Cybersecurity Authority.

7. The National Cybersecurity Authority shall notify the European Commission, without delay, of the identity of the CSIRTs of paragraph 1, any other CSIRTs designated by the decision of paragraph 8 of article 30, their respective tasks in relation to key and important entities, the CSIRT to which coordination tasks are assigned in accordance with this article, as well as any subsequent changes.

Article 11
Requirements, technical capabilities and tasks of computer security incident response teams (CSIRTs)
(Article 11 of Directive (EU) 2022/2555)

1. Computer Security Incident Response Teams (CSIRTs) shall comply with the following requirements:

a) ensure a high level of availability of their communication channels, avoiding single points of failure and have alternative ways for incoming and outgoing communication with third parties at all times, clearly identify the communication channels and communicate them to the members of their area of responsibility and to cooperating partners,

b) the CSIRTs' facilities and supporting information systems are located in secure areas,

c) CSIRTs are equipped with an appropriate request management and routing system, in particular in order to facilitate the effective and efficient performance of tasks,

d) CSIRTs ensure the confidentiality and reliability of their activities,

e) CSIRTs are adequately staffed to ensure the availability of their services at all times and ensure that their personnel are appropriately trained,

f) CSIRTs are equipped with backup systems and a backup workspace to ensure the continuity of their services.

The CSIRT of the National Cybersecurity Authority, as well as other CSIRTs, may participate in international cooperation networks. In particular, the CSIRT of the National Cybersecurity Authority may be assisted by other CSIRTs for its participation in the above networks.

2. CSIRTs are tasked with the following tasks:

a) monitoring and analysis of cyber threats, vulnerabilities and incidents at national level, exclusively for the sectors and organisations under their responsibility and, upon request, providing assistance to affected key and important entities regarding the monitoring of their network and information systems in real time or near real time;

b) providing timely warnings, alerts, announcements and information to key and important entities involved, as well as to competent authorities and other relevant stakeholders regarding cyber threats, vulnerabilities and incidents, if possible in near real time,

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

d) collection and analysis of forensic data and dynamic analysis of risks and incidents and awareness of the situation in cybersecurity matters,

(e) providing, upon request of a key or significant entity, a proactive scan of the network and information systems of that entity to identify vulnerabilities with a potential significant impact;

f) participation, following a decision of the Director of the National Cybersecurity Authority, in the CSIRTs network of Article 15 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (L 333) providing mutual assistance in accordance with their capabilities and responsibilities to other members of the CSIRTs network upon their request,

g) contribution to the development of secure information exchange tools in accordance with paragraph 4 of article 10.

CSIRTs may conduct proactive non-intrusive scanning of publicly accessible network and information systems of key and important entities, provided that it does not have a negative impact on the operation of the entities' services. Such scanning is carried out to identify vulnerable or insecurely configured network and information systems and to inform the entities concerned.

When carrying out the tasks referred to in the first subparagraph, CSIRTs may prioritise specific tasks within the framework of a risk-based approach.

3. CSIRTs may cooperate with interested parties in the private sector, with a view to achieving the objectives of this law. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standard practices, classification systems and taxonomies in relation to:

a) incident management procedures,

b) crisis management, and

c) coordinated vulnerability disclosure in accordance with paragraph 1 of article 12.

Article 12
Coordinated vulnerability disclosure and European vulnerability database (article 12 of Directive 2022/2555)

1. The CSIRT of the National Cybersecurity Authority is assigned the coordinating role for the purposes of coordinated vulnerability disclosure. The aforementioned CSIRT acts as a trusted intermediary, facilitating, where necessary, communication between the natural or legal person reporting the vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon request of one of the parties. The tasks of the aforementioned CSIRT to which the coordinating role has been assigned include:

a) the identification of the relevant entities and communication with them,

b) providing assistance to natural or legal persons who report vulnerabilities, and

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

2. Natural or legal persons may , upon request, anonymously report vulnerabilities to the CSIRT referred to in paragraph 1. That CSIRT shall ensure that diligent follow-up actions are carried out in relation to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. In cases where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT referred to in paragraph 1 shall cooperate, as appropriate, with other CSIRTs to which a coordination role has been assigned within the CSIRTs network.

Article 13
Cooperation at national level
(Article 13 of Directive (EU) 2022/2555)

1. The National Cybersecurity Authority, as the competent authority, single point of contact and response team for incidents related to computer security (CSIRT), as well as the CSIRTs of paragraphs 1 and 2 of article 10, cooperate with each other to comply with the obligations provided for in this law.

2. CSIRTs shall receive reports of serious incidents in accordance with Article 16, as well as of cyberthreat incidents and near-misses in accordance with Article 22. CSIRTs shall inform, without delay, the CSIRT of the National Cybersecurity Authority of notifications of cyberthreat incidents and near-misses submitted in accordance with this law.

3. The National Cybersecurity Authority, the CSIRTs and the other competent national authorities systematically exchange information with each other with the aim of more effectively performing their duties, and in particular:

a) The National Cybersecurity Authority shall notify each competent CSIRT of the data submitted to it in accordance with paragraphs 3 and 4 of article 4.

b) Each competent CSIRT, which is involved in an incident, informs, without delay and no later than twenty-four (24) hours, the CSIRT of the National Cybersecurity Authority and communicates a relevant report, as well as any other requested information within seventy-two (72) hours.

c) To the Coordination Committee for Cybersecurity Issues security are sent:

ca) the data communicated in accordance with paragraph 5 of article 4, paragraph 3 of article 9 and paragraph 6 of article 16 hereof and

cb) the necessary data and reports regarding the progress of implementation of the National Cybersecurity Strategy .

d) The Coordination Committee for Cybersecurity Issues, within the framework of the execution of its responsibilities, the National Cybersecurity Authority and the bodies defined in paragraph 1 of article 26 of law 5002/2022 are obliged to cooperate and exchange information, in particular with regard to the management of an incident involving a strategic risk, in accordance with paragraph a) of article 22 of law 5002/2022.

4. In order to ensure the effective execution of the tasks and obligations of the National Cybersecurity Authority as a competent authority, single point of contact and CSIRT, as well as the other
CSIRTs, these bodies and the competent law enforcement authorities, the Personal Data Protection Authority , the Communications Privacy Authority, the competent national authorities designated in accordance with Regulation (EC) 300/2008 of the European Parliament and of the Council of 11 March 2008 on the establishment of common rules in the field of civil aviation security and the abolition of Regulation (EC) 2320/2002 (L 97) and Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) 2111/2005, (EC) 1008/2008, (EU) 996/2010, (EU) 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) 552/2004 and (EC) 216/2008 of the European Community. Parliament and of the Council and Council Regulation (EEC) No 3922/91 (L 212), the supervisory bodies designated in accordance with 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 (L 257), the competent authorities designated in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 (L 333), the national regulatory authorities designated in accordance with Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (L 321), the competent authorities designated in accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (L 333), as well as the competent authorities designated in accordance with other sectoral legal acts of the European Union , within the country.

5. The National Cybersecurity Authority, as the competent national authority under this law, and the other competent national authorities under Directive (EU) 2022/2557, shall cooperate and exchange information on a regular basis regarding the identification of critical entities, risks, cyber threats and incidents, as well as risks, threats and incidents outside cyberspace, affecting key entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken to address such risks, threats and incidents. The above competent authorities and the competent authorities designated in accordance with Regulation (EU) 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 shall exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats.

6. It is possible to designate authorities, bodies, services or organic units of the public administration with regulatory and supervisory responsibilities in individual

sectors of Annexes I and II, as sectoral points of contact and cooperation at national level with the National Cybersecurity Authority (National Sectorial Focal Points, NSFPs) in accordance with paragraph 11 of article 30. The NSFPs are obliged in particular to inform and provide, without delay, any necessary assistance to the National Cybersecurity Authority for the response and management of cybersecurity incidents, as well as to participate in Cooperation Groups on cybersecurity issues, which are established by the National Cybersecurity Authority, with the aim of deepening cooperation at national level for the acceleration of the purposes of this

CHAPTER D
RISK MANAGEMENT MEASURES IN THE SECTOR CYBERSECURITY AND OBLIGATIONS INCIDENT REPORTING

Article 14
Governance
(Article 20 of Directive (EU) 2022/2555)

1. The management bodies of key and significant entities shall, within three (3) months from the entry into force of this Regulation, approve the cybersecurity risk management measures taken by these entities to comply with Article 15, monitor their implementation and be liable for any breach by the entities of the obligations of this Regulation. This Regulation shall not affect the applicable rules on liability of public administration entities, as well as the liability of public officials and elected or appointed officials.

2. Members of the management bodies of key and significant entities shall attend training and ensure that key and significant entities provide similar training to their employees at least on an annual basis, in order to acquire sufficient knowledge and skills that allow them to identify risks and assess risk management practices in the field of cybersecurity and their impact on the services provided by the entity.

Article 15
Risk management measures in the sector cybersecurity
(article 21 and paragraph 1 of article 24 of Directive (EU) 2022/2555)

1. Key and significant entities shall take appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of network and information systems that they use for their activities or for the provision of their services and to prevent or minimise the impact of incidents on the recipients of their services or on other services and organisations. Taking into account the most up-to-date and, where appropriate, relevant national, European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems proportionate to the risk involved. When assessing the proportionality of those measures, account shall be taken of the entity's exposure to risks, the size of the entity, the likelihood of incidents occurring and their severity, including their social and economic impact.

2. The measures referred to in paragraph 1 shall be based on a holistic risk approach aimed at protecting network and information systems and the physical environment of such systems from incidents, and shall include at least the following:

a) policies and procedures for risk analysis and the security of information systems,
b) incident management,
c) business continuity, such as backup management and disaster recovery , as well as crisis management,

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

e) security in the acquisition, development and maintenance of network and information systems, including the handling and disclosure of vulnerabilities,

f) policies and procedures for assessing the effectiveness of risk management measures in the field of cybersecurity,
g) basic cyber hygiene practices and training in cybersecurity,
h) policies and procedures regarding the use of cryptography and, where applicable, encryption, in cooperation with the national CRYPTO authority, where required,
i) human resources security, control policies access and management of fixed assets,
j) use of multi-factor authentication or continuous authentication solutions, secure voice communications, video and text communications and secure emergency communications systems within the entity, as appropriate.

3. If the measures referred to in point d) of paragraph 2 are deemed, in accordance with the decision of paragraph 15 of article 30, to be appropriate, entities shall take into account the vulnerabilities that characterize each direct supplier and service provider, the overall quality of the products and cybersecurity practices of their suppliers and service providers, including their secure development processes, as well as the results of the coordinated risk assessments of critical supply chains carried out in accordance with paragraph 1 of article 22 of Directive 2022/2555.

4. Any entity that is found not to be complying with the measures provided for in paragraph 2 shall be subject to

shall, without delay, take all necessary, appropriate and proportionate corrective measures.

5. The basic and important entities:

a) They appoint a competent executive, with appropriate qualifications and expertise, as the Information and Communications Systems Security Officer (ICSSO), who undertakes:

aa) the management of all types of communications and in collaboration with the National Cybersecurity Authority,

(bb) the diligence and internal coordination for the compliance of the entity concerned with the requirements of this article, as well as the reporting requirements in accordance with article 16.

The DPO shall be provided by the relevant entity with the necessary resources for the performance of its duties. The duties of the DPO are incompatible with those of the Data Protection Officer (DPO) of Article 37 of 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 (General Data Protection Regulation, L 119) and Articles 7 and 8 of Law 4624/2019 (Government Gazette A' 137). The DPO shall has an appropriate level of autonomy in decision-making , the ability to implement them by the individual organizational units of the entity, the information of the administrative bodies, the coordination of security incident management , as well as the implementation procedures of business continuity and disaster recovery plans. For central government bodies, as defined in paragraph c of paragraph 1 of article 14 of law 4270/2014 (Government Gazette A' 143), articles 18 and 19 of law 4961/2022 (Government Gazette A' 146) apply, regarding the definition, qualifications and duties of the Y.A.S.P.E.

b) They shall comply with a unified cybersecurity policy, in accordance with the standardized template of paragraph 14 of article 30, which includes all of the individual measures, policies and procedures of paragraph 2 hereof. In the event that the entity complies with individual recorded policies and procedures, which concern at least the compliance measures of paragraph 2 hereof, the unified cybersecurity policy shall refer to these policies and procedures for the individual details. The unified cybersecurity policy shall be submitted for approval in terms of its completeness by the basic entities to the National Cybersecurity Authority, at least annually. The submission of the unified cybersecurity policy by the significant entities may be mandatory by decision of paragraph 15 of article 30. A prerequisite for examining the unified policy is the payment of the supervision fee of par. 1 of article 23.

c) They maintain a comprehensive record of tangible and intangible information and communication assets, which are prioritized based on their criticality.

6. In order to demonstrate compliance with the requirements of paragraphs 1 and 2, key and significant entities may be required to use specific ICT products, ICT services and ICT processes, developed by the key or significant entity or provided by third parties and certified under European cybersecurity certification schemes established in accordance with Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the " European Union Agency for Cybersecurity") and on cybersecurity certification in the information and communications technology sector and repealing Regulation (EU) 526/2013 (Cybersecurity Act, L 151). Measures may also be provided to encourage key and important entities to use approved trust services.

Article 16
Incident reporting obligations
(article 23 of Directive 2022/2555)

1. The key and significant entities shall notify, without delay, the Computer Security Incident Response Team (CSIRT) of the National Cybersecurity Authority of any incident that has a significant impact on the provision of their services, in accordance with paragraph 3 (significant incident). The entities referred to in paragraph f) of paragraph 2 of Article 3 shall notify the incidents of this Article to the
CSIRT of the National Intelligence Service with simultaneous notification of the National Cybersecurity Authority . Where appropriate, the entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that may negatively affect the provision of such services. Such entities shall report, inter alia , any information that allows the National Cybersecurity Authority to determine the cross-border implications of the incident. The mere act of notification shall not entail liability of the notifying entity. In the event of a cross-border or cross-sectoral significant incident, the National Cybersecurity Authority shall provide, without delay, to the single points of contact referred to in paragraph 8 the relevant information communicated to it in accordance with paragraph 4.

2. Key and significant entities shall, without delay, notify the relevant recipients of their services who may be affected by a significant cyber threat of measures or corrective actions that they can take to address the specific threat. The entities shall also inform those recipients of the significant cyber threat.

3. An incident is considered significant if:

a) has caused or may cause serious operational disruption of services or financial damage to the entity concerned,

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

4. For the notification of paragraph 1, the relevant entities submit to the National Cybersecurity Authority:

a) without undue delay and in any case within twenty-four (24) hours of becoming aware of the significant incident, a warning, which, where appropriate, states whether there is a suspicion that the significant incident was caused by illegal or malicious actions or could have a cross-border impact,

b) without undue delay and in any case within seventy-two (72) hours of becoming aware of the significant incident, an incident report, which, where appropriate, updates the information referred to in point a) and, in addition, includes an initial assessment of the significant incident, including its severity and impact, as well as, if any, the indications of the breach,

c) upon request of the National Cybersecurity Authority , an interim report on relevant updates of the situation,

d) a final report no later than one (1) month after the submission of the incident notification in accordance with paragraph b), which includes the following:

(da) a detailed description of the incident, including its severity and impact; (db) the type of threat or root cause that may have caused the incident; (dc) implemented and ongoing mitigation measures; (dd) where applicable, the cross-border impact of the incident;

e) in the event of an ongoing incident at the time of submission of the final report referred to in paragraph d), the relevant entities shall submit a progress report at that time and a final report within one (1) month of their handling of the significant incident.

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

5. The National Cybersecurity Authority shall provide the notifying entity, without delay and if possible within twenty-four (24) hours of receipt of the early warning referred to in point a) of paragraph 4, with a response including an initial response to the significant incident and, upon request by the entity, guidance or operational advice on the implementation of possible mitigation measures. The National Cybersecurity Authority shall provide additional technical support, if requested by the entity concerned. Where there are suspicions that the significant incident is of a criminal nature, the National Cybersecurity Authority shall The Security Service also provides guidance on reporting the significant incident to the competent prosecution authorities or to the competent Directorate of the Hellenic Police.

6. Where appropriate, and in particular where the significant incident also concerns other Member States of the European Union, the CSIRT of the National Cybersecurity Authority shall, without delay, inform the other affected Member States and the European Union Agency for Cybersecurity (ENISA) of the significant incident. This information shall include the type of information received in accordance with paragraph 4. In this context, the National Cybersecurity Authority shall safeguard, in accordance with Union and national law, the security and commercial interests of the entity, as well as the confidentiality of the information provided.

7. Where public awareness is necessary to prevent a significant incident or to address a significant ongoing incident, or where disclosure of the significant incident is in the public interest, the National Cybersecurity Authority may, after consultation with the entity concerned, inform the public about the significant incident or require the entity to inform the public within a specified period.

8. The National Cybersecurity Authority shall forward the notifications it receives in accordance with paragraph 1 to the single points of contact of any other affected Member States of the European Union.

9. The National Cybersecurity Authority, as a single point of contact, shall submit to ENISA, every three (3) months, a summary report, which includes anonymized and aggregated data on significant incidents , incidents, cyber threats and near misses notified in accordance with paragraph 1 of this and article 22.

10. The National Cybersecurity Authority shall provide the competent authorities, designated in accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, on the resilience of critical entities and repealing Council Directive 2008/114/EC (L 333), with information on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Regulation and Article 22 by entities identified as critical entities in accordance with Directive (EU) 2022/2557.

Article 17
Standardization
(Article 25 of Directive (EU) 2022/2555)

For the effective implementation of paragraphs 1 and 2 of article 15, it may be provided, by decision of the Director of the National Cybersecurity Authority and after taking into account any guidelines issued by the European Union Agency for Cybersecurity (ENISA), without imposing or favoring the use of a specific type of technology, that

establishing measures to encourage the use of European and internationally accepted standards and technical specifications relating to the security of network and information systems.

CHAPTER E
JURISDICTION AND REGISTRATION

Article 18
Jurisdiction and territoriality
(Article 26 of Directive (EU) 2022/2555)

1. Entities established or providing services or carrying out activities in the country and falling within the scope of this Part shall be deemed to be subject to its jurisdiction, unless:

a) providers of public electronic communications networks or providers of publicly available electronic communications services, which are considered to fall under the jurisdiction of another Member State of the European Union in which they provide their services,

(b) Domain Name System (DNS) service providers, top-level domain (TLD) registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content distribution network providers, managed service providers, managed security service providers, as well as online/

online marketplaces, online/web search engines or social networking service platforms, which are considered to fall under the jurisdiction of another Member State of the European Union in which they have their main establishment in accordance with paragraph 2,

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

2. For the purposes of this Part, an entity referred to in point (b) of paragraph 1 shall be deemed to have its main establishment in the territory of the Member State where the decisions relating to risk management measures in the field of cybersecurity are mainly taken. If the Member State cannot be determined in accordance with the previous paragraph, the main establishment shall be deemed to be located in the territory of the Member State where the cybersecurity operations are carried out . If the Member State cannot be determined in accordance with the previous paragraph, the main establishment shall be deemed to be located in the territory of the Member State where the entity concerned has in Greece the establishment with the largest number of employees in the European Union.

3. If an entity referred to in paragraph b) of paragraph 1 is not established in the European Union, but offers services within it, it must appoint a representative in the European Union. Such an entity is considered to be subject to the jurisdiction of Greece if the representative is established there . In the absence of a representative, in accordance with this, In the European Union, the entity providing services in Greece is liable for breach of the obligations of this part.

4. The appointment of a representative by an entity referred to in point b) of paragraph 1 does not affect the legal actions that may be taken against the entity itself.

5. If a request for mutual assistance is submitted to the National Cybersecurity Authority in relation to an entity referred to in paragraph 1, the competent authorities under this Part shall take, within the limits of the said request, appropriate supervisory and enforcement measures in relation to the entity concerned, which provides services or has the network and information system in the Greek territory.

Article 19
Entity registry
(Article 27 of Directive (EU) 2022/2555)

1. Domain Name System (DNS) service providers , top-level domain name (TLD) registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content distribution network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines or social networking service platforms , shall mandatorily submit to the National Cybersecurity Authority , no later than 17 January 2025, the following information:

a) the name of the entity,

(b) the relevant sector, subsector and type of entity referred to in Annexes I and II, as appropriate ;

c) the address of the entity's main establishment and its other legal establishments in the European Union or, if it is not established therein , the address of its representative, who has been designated in accordance with paragraph 3 of Article 18,

d) up-to-date contact details, including e-mail addresses and telephone numbers of the entity and, where applicable, of its representative, who has been designated in accordance with paragraph 3 of Article 18;

e) the Member States in which the entity provides services and

f) the Internet Protocol (IP) range of the entity.

2. The entities referred to in paragraph 1 shall notify the National Cybersecurity Authority, without delay and, in any case, within three (3) months from the date of occurrence of the change, of changes to the information they submitted.

3. Upon receipt of the information referred to in paragraphs 1 and 2, except for the information referred to in point f) of paragraph 1, the National Cybersecurity Authority shall transmit it to the European Union Agency for Cybersecurity (ENISA).

Article 20
Domain name registration database
(Article 28 of Directive (EU) 2022/2555)

1. For the security, stability and resilience of the Domain Name System (DNS), top-level domain (TLD) registries and entities providing domain name registration services shall collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with 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 (General Data Protection Regulation, L 119) GDPR and the

Law 4624/2019 (A' 137).

2. For the purposes of paragraph 1, the domain name registration database shall contain the information necessary to identify and communicate with domain name holders and the contact points managing domain names under the TLDs. This information shall include:

a) the domain name,
b) the date of registration,
c) name, contact email address and the registrant's telephone number,
d) the contact email address and telephone number of the point of contact managing the domain name, if different from those of the registrant.

3. TLD name registries and entities providing domain name registration services shall have policies and procedures, including verification procedures, to ensure that the databases referred to in paragraph 1 contain accurate and complete information.

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

5. TLD registries and entities providing domain name registration services shall provide access to specific domain name registration data upon lawful and duly justified requests from legitimate access seekers, in accordance with 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 (General Data Protection Regulation, L 119) GDPR and the

Law 4624/2019 (A' 137). The TLD name registries and Entities providing domain name registration services shall respond without undue delay and in any event within seventy-two (72) hours of receipt of any access requests. They shall also make public the policies and procedures for disclosing such data.

6. Compliance with the obligations set out herein shall not result in duplication of the collection of domain name registration data. To this end, TLD registries and entities providing domain name registration services shall cooperate with each other.

CHAPTER FIVE
INFORMATION EXCHANGE

Article 21
Arrangements for information exchange in the field of cybersecurity
(Article 29 of Directive (EU) 2022/2555)

1. Entities falling within the scope of this Part and, where appropriate, other entities not falling within its scope , shall exchange with each other, on a voluntary basis, information relevant to cybersecurity, including information on cyber threats, near-misses, vulnerabilities, techniques and procedures, indications of breach, malicious tactics, information on specific threat actors, cybersecurity alerts and recommendations on the configuration of cybersecurity tools to detect cyber-attacks, to the extent that such exchange of information:

a) aims to prevent, detect, respond to or recover from incidents or mitigate their effects,

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

2. Information exchange shall take place within communities of key and significant entities and, where appropriate, their suppliers or service providers. Such exchange shall take place taking into account the potentially sensitive nature of the information exchanged.

3. The key and significant entities shall notify the National Cybersecurity Authority, without delay, of their participation in the information exchange framework of par. 2, as well as the withdrawal of their participation, once this has taken place.

Article 22
Voluntary disclosure of relevant information
(Article 30 of Directive (EU) 2022/2555)

1. In addition to the notification obligation provided for in article 16, notifications may be submitted to the National Cybersecurity Authority on a voluntary basis, by:

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

2. The National Cybersecurity Authority shall process the notifications referred to in paragraph 1 in accordance with the procedure laid down in Article 16, giving priority to the processing of mandatory notifications over voluntary notifications. The National Cybersecurity Authority shall ensure the confidentiality and appropriate protection of the information provided by the reporting entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not impose additional obligations on the reporting entity which it would not have been subject to if it had not submitted the notification.

CHAPTER G'
SUPERVISION AND SANCTIONS

Article 23
General aspects concerning supervision and enforcement
(paragraph 5 of article 8, paragraph 1 of article 9, paragraph 2 of article 10, paragraph 2 of article 11 and article 31 of Directive (EU) 2022/2555)

1. The National Cybersecurity Authority is designated as the competent supervisory and control authority for compliance with the provisions of this part and exercises supervision and control in accordance with articles 24 and 25.
Entities under the supervision of the National Cybersecurity Authority, with the exception of entities under point f) of paragraph 2 of article 3, are subject to a proportional supervision fee and a proportional audit fee, based in particular on the size of the entity and the complexity of the audit, which are determined by the joint decision of paragraph 20 of article 30.
The assignment of control and inspection tasks and the designation of certified technical experts (Subject Matter Experts, SMEs) is carried out in accordance with paragraph 21 of article 30. In particular, the supervision of the entities of paragraph 2 of article 3 is exercised exclusively by the inspectors of the National Cybersecurity Authority and by inspectors of the public administration certified by it , who may, where appropriate, be assisted by an SME certified by the National Cybersecurity Authority, in accordance with the Regulation Control and Supervision of the National Cybersecurity Authority. In the event of the designation and exercise of supervisory responsibilities by National Sectorial Focal Points (NSFP) in accordance with paragraph 11 of article 30, supervision and control duties in accordance with the provisions of this law are exercised by the inspectors of the National Cybersecurity Authority and the inspectors of the National Sectorial Focal Points (NSFP) certified by the National Cybersecurity Authority . The bodies participating in the control process, including the certified inspectors and the certified technical experts, receive compensation, the amount of which is determined by the decision of paragraph 20 of article 30.

2. The revenues from the financial sanctions imposed on natural or legal persons in accordance with this Part, as well as from the supervision fee and the control fee of par. 1, constitute resources of the National Cybersecurity Authority and are allocated exclusively to cover its operating expenses and to serve the purposes of its operation.

3. The National Cybersecurity Authority cooperates with the Personal Data Protection Authority in dealing with incidents leading to personal data breaches, without prejudice to the competence and duties of the Personal Data Protection Authority in accordance with 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.

EC (General Data Protection Regulation, L 119).

4. In case of violation of the provisions of this Part, the fines provided for in article 26 and in paragraph 23 of article 30 shall be imposed, as appropriate.

5. The bodies of the National Cybersecurity Authority enjoy, vis-à-vis the supervised public administration bodies, operational independence in the exercise of their supervisory and control responsibilities provided for in this article and in articles 24 to 27 and 30.

6. In order to fulfill the duties of the National Cybersecurity Authority, as provided for herein , its authorized employees have supervisory powers and have the authority, in particular:

a. to visit, in the context of the exercise of their duties and for the fulfillment of their work, with or without notice, the entities that fall within the scope of this Regulation,

b. to control and collect information and data from mobile terminals, portable devices, their servers and the cloud, in cooperation with the competent authorities, as the case may be, located inside or outside the buildings of these controlled entities,

c. to conduct investigations in offices and other entity spaces,
d. to seize, receive or obtain in any form a copy or extract of books, documents, as well as electronic data storage and transfer media, which relate to professional information and, when they deem it appropriate, to continue the search for information and select copies or extracts at the premises of the National Cybersecurity Authority or at other designated premises,

e. to seal any business premises, electronic or non-electronic books or documents, during the period in which the audit is being carried out and to the extent necessary.

Article 24
Supervisory and enforcement measures in relation to with basic entities
(Article 32 of Directive (EU) 2022/2555)

1. Supervisory or enforcement measures imposed on key entities in relation to the obligations set out in this Part shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.
2. The National Cybersecurity Authority, when exercising its supervisory duties in relation to key entities, has the competence to subject such entities to procedures concerning:
a) on-site inspections and supervision outside the premises, including sampling checks, carried out by the inspectors referred to in paragraph 1 of Article 23,

b) regular and targeted security audits carried out by the National Cybersecurity Authority,
c) extraordinary special inspections, inter alia, when this is justified due to a significant incident or violation of this law by the main entity or when a relevant complaint has been submitted or there is information or circumstantial evidence of the existence of such an incident or violation,
d) security scans based on objective, impartial, fair and transparent risk assessment criteria, where required with the cooperation of the entity concerned,

e) requests for the provision of necessary information for the ex-post evaluation of the cybersecurity risk management measures taken by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to transmit information to the National Cybersecurity Authority,
f) requests for access to data, documents and information required for the performance of its supervisory tasks,
g) requests for evidence concerning the implementation of cybersecurity policies, such as the results of security audits carried out by an authorized inspector of par. 1 of article 23 and the corresponding underlying evidence .

The targeted security audits of paragraph b) are based on risk assessments, carried out by the National Cybersecurity Authority or the audited entity, or on other risk-related information available.

The results of each targeted security audit are made available to the competent Directorate of the National Cybersecurity Authority.
3. The National Cybersecurity Authority, when exercising the powers of paragraphs e), f) and g) of paragraph 2, shall state the purpose of the request and specify the information requested.
4. The National Cybersecurity Authority, when exercising its supervisory duties in relation to key entities, has the following responsibilities:
(a) issue warnings or recommendations regarding violations of this Part by the entities concerned ;

(b) issue binding instructions and guidelines, inter alia, regarding the measures necessary to prevent or remedy an incident, and set deadlines for the implementation of such measures and for reporting on their implementation, or order the entities concerned to remedy the deficiencies identified or the violations of this Part;

(c) order the entities concerned to cease conduct in breach of this Part and to refrain from repeating such conduct;
(d) order the entities concerned to ensure that cybersecurity risk management measures comply with Article 15 or to fulfil the reporting obligations set out in Article 16, in a specific manner and within a specified period of time;

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

(f) instruct the entities concerned to implement the recommendations made as a result of a security audit within a reasonable period of time;
g) appoint a competent supervisor with clearly defined tasks for a specified period of time, in order to supervise the compliance of the entities concerned with Articles 15 and 16,
h) orders the relevant entities to make public information on violations of this part in a specific manner and procedure,
i) imposes administrative fines in accordance with the article Article 26, in addition to the measures in paragraphs a) to h).
5. Where the enforcement measures adopted in accordance with paragraphs a) to d) and f) of paragraph 4 are deemed to be

effectively, the National Cybersecurity Authority sets a deadline within which the main entity is required to take the necessary measures to remedy the deficiencies or to comply with it. If the requested measures are not taken within the specified deadline , the Director of the National Cybersecurity Authority, upon recommendation of the competent organizational unit, may, by a specifically reasoned decision:

a) temporarily suspend or request the competent certification body to suspend the certification or authorization concerning part or all of the relevant services provided or activities performed by the main entity,

(b) temporarily prohibit any natural person who is responsible for exercising management functions at the level of managing director or legal representative in the main entity from exercising management functions in that entity.

The temporary suspensions or prohibitions imposed pursuant to this shall be valid only until the entity concerned has taken the necessary measures to remedy the deficiencies or to comply with the requirements of the above competent authority for which such enforcement measures were applied. An application for annulment may be filed before the Council of State against the decision of the Governor of the National Cybersecurity Authority imposing a temporary suspension or prohibition. The above decision of the Governor of the National Cybersecurity Authority may be revoked, provided that the entity complies.

The enforcement measures provided for herein do not apply to the entities referred to in point (f) of paragraph 2 of article 3 that are subject to this Part.

6. Any natural person who, in accordance with the applicable legislation, is, as the case may be, responsible for or acts as the legal representative of a basic entity based on its power of representation or has the power to take decisions on its behalf or to exercise control over it, shall be responsible for ensuring its compliance with this law. Such natural persons shall be held liable for the breach of their obligations under this law. The application of this law shall not affect the existing provisions on liability applicable to public administration entities , as well as on the liability of public officials and elected or appointed members of their administration.

7. The National Cybersecurity Authority, when taking any of the enforcement measures referred to in paragraphs 4 and 5, shall take into account the circumstances of each individual case. In particular, it shall take due account of:

a) the seriousness of the violation and the importance of the provisions violated. Serious violations are considered in any case in particular: aa) repeated violations, ab) failure to notify or remedy significant incidents, ag) failure to remedy deficiencies in accordance with binding instructions from the competent authorities in each case, ad) obstruction of controls or supervision activities ordered by the National Cybersecurity Authority following the detection of a breach, ae) providing false or grossly inaccurate information in relation to the risk management measures or reporting obligations set out in Articles 15 and 16,

b) the duration of the infringement,

c) relevant previous violations by the entity concerned,

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

e) any fault on the part of the perpetrator of the violation,

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

g) any compliance with approved codes of ethics or approved certification mechanisms,

h) the degree of cooperation of the natural or legal persons responsible with the competent authorities.

8. The National Cybersecurity Authority shall justify the enforcement measures and, before taking them, shall notify the entities concerned of its preliminary findings and any warnings. It shall provide a reasonable period of time, in the circumstances, for the entities concerned to submit observations, except in justified cases where taking immediate action to prevent or respond to incidents would otherwise be prevented.

9. The National Cybersecurity Authority shall inform the authorities exercising relevant responsibilities, as the case may be, when exercising their supervisory and enforcement powers in accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (L 333), with the aim of ensuring the compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with the obligations of this Part . The competent authorities designated in accordance with Directive (EU) 2022/2557 may request, in accordance with this Part, the National Cybersecurity Authority to exercise its supervisory and enforcement powers in relation to an entity identified as a critical entity under Directive (EU) 2022/2557.

10. The National Cybersecurity Authority shall cooperate with the national competent authorities designated in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 (L 333). In particular, the National Cybersecurity Authority shall inform the supervisory forum established in accordance with paragraph 1 of Article 32 of Regulation (EU) 2022/2554 during the

exercise of its supervisory and enforcement powers aimed at ensuring compliance of a key entity, designated as a critical third party provider of information and communication technology (ICT) services in accordance with Article 31 of Regulation (EU) 2022/2554, with the obligations of this law.

Article 25
Supervisory and enforcement measures in relation to with important entities
(Article 33 of Directive (EU) 2022/2555)

1. The National Cybersecurity Authority, when provided with evidence, indications or information that a significant entity is suspected of not complying with this Part, in particular with Articles 15 and 16 thereof, shall take, if it deems it necessary, repressive measures, which must be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. The National Cybersecurity Authority, when exercising its enforcement powers in relation to significant entities, shall subject such entities in particular to the following:

a) on-site inspections and repressive supervision inside and outside the premises,

b) targeted security checks carried out by are provided by the National Cybersecurity Authority,

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

(d) requests for information necessary for the assessment of the cybersecurity risk management measures taken by the entity concerned , including documented cybersecurity policies, as well as compliance with the obligation to transmit information to the competent authorities in accordance with Article 19;

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

f) requests for evidence concerning the implementation of cybersecurity policies, such as the results of security audits carried out by an authorized inspector of paragraph 1 of article 23 and the corresponding underlying evidence .

The targeted security audits referred to in paragraph b) are based on risk assessments carried out by the National Cybersecurity Authority or the audited entity or on other available information regarding risks.

The results of each targeted security audit are made available to the competent organizational unit of the National Cybersecurity Authority.

3. When exercising its powers in accordance with paragraphs d), e) and f) of paragraph 2, the National Cybersecurity Authority shall state the purpose of the request and specify the information requested.

4. The National Cybersecurity Authority, when exercising its supervisory powers in relation to significant entities, has in particular the following powers:

(a) issue warnings or recommendations regarding violations of this Part by the entities concerned;

b) issues binding instructions or an order to the relevant entities to remedy the identified deficiencies or the violation of the obligations of this Part,

(c) order the entities concerned to cease conduct that violates this Part and to refrain from repeating such infringing conduct;

(d) order the entities concerned to ensure that cybersecurity risk management measures comply with Article 15 or to fulfil the reporting obligations set out in Article 16, in a specific manner and within a specified period of time;

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

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

g) orders the relevant entities to disclose aspects of violations of this Part in a specific manner,

h) impose administrative fines in accordance with Article 26, in addition to the measures referred to in paragraphs a) to g).

5. Paragraphs 6, 7, 8 and 10 of article 24 shall apply mutatis mutandis to the supervisory and enforcement measures provided for in this article for significant entities .

Article 26
General conditions for the imposition of administrative fines on key and significant entities - Sanctions
(Articles 34 and 36 of Directive (EU) 2022/2555)

1. Supervisory or enforcement measures imposed on key or significant entities in relation to this Part shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Sanctions against natural or legal persons for the violation of the provisions of this article shall be imposed by a specifically reasoned decision of the Director of the National Cybersecurity Authority, which shall be issued after a hearing following their summons, in accordance with article 6 of the Code of Administrative Procedure (Law 2690/1999, A' 45). By the decision of par. 23 of article 30, the following may be imposed:

road financial sanctions to key or significant entities, in order to compel them to cease a violation of this Part in accordance with a previous decision of the National Cybersecurity Authority.

3. Decisions imposing fines and sanctions shall be notified to the interested parties and shall be posted, without delay, on the official website of the National Cybersecurity Authority . Decisions imposing fines and any other type of sanctions shall be appealed by means of an application for annulment to the competent Administrative Court of Appeal.

4. If a breach of Articles 15 or 16 is found, a fine of up to ten million (10,000,000) euros or up to two percent (2%) of the total worldwide annual turnover of the undertaking to which the significant entity belongs in the preceding financial year shall be imposed on the significant entities, whichever is higher.

5. If a breach of Articles 15 or 16 is found, a fine of up to seven million (7,000,000) euros or up to one point four percent (1.4%) of the total worldwide annual turnover of the undertaking to which the significant entity belongs in the preceding financial year shall be imposed on the significant entities, whichever is higher.

6. Administrative fines shall be imposed, in addition to the measures referred to in paragraphs a) to h) of paragraph 4 and paragraph 5 of article 24, as well as in paragraphs a) to g) of paragraph 4 of article 25, for the violation of paragraphs a) to h) of paragraph 4 and paragraph 5 of article 24, of a maximum amount of one million (1,000,000) euros, and for the violation of paragraphs a) to g) of paragraph 4 of article 25, of a maximum amount of seven hundred thousand (700,000) euros.

7. When making a decision regarding the imposition of an administrative fine and its amount, the elements provided for in paragraph 7 of article 24 shall be taken into account, at a minimum.

8. Without prejudice to the powers of the National Cybersecurity Authority in accordance with Articles 24 and 25, administrative fines shall be imposed on the entities referred to in point (f) of paragraph 2 of Article 3 that are subject to the obligations set out in this Part. Such fines may not be less than twenty thousand (20,000) euros and may not exceed five hundred thousand (500,000) euros.

9. If a violation is detected:

a) of paragraph 1 of article 14, a fine of a maximum of two hundred thousand (200,000) euros shall be imposed,

b) of paragraph 2 of article 14, a fine of a maximum of one hundred thousand (100,000) euros shall be imposed,

c) of article 19, a fine of

a maximum limit of two hundred thousand (200,000) euros,

d) of article 20, a fine of

a maximum limit of eight hundred thousand (800,000) euros,

e) of paragraph 3 of article 21, a fine of a maximum of one hundred thousand (100,000) euros shall be imposed,

f) of paragraphs 2 and 4 of article 24, a fine of a maximum of five hundred thousand (500,000) euros shall be imposed,

g) of paragraph 2 of article 25, a fine of a maximum of three hundred and fifty (350,000) euros shall be imposed, and

h) of paragraph 6 of article 15, a fine of a maximum of three hundred thousand (300,000) euros shall be imposed.

Article 27
Breaches involving a breach of personal data
(Article 35 of Directive (EU) 2022/2555)

1. If the National Cybersecurity Authority finds, in the context of supervision or the imposition of sanctions, that the breach by a key or significant entity of the obligations set out in Articles 15 and 16 may entail a breach of personal data , as defined in point 12) of Article 4 of 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 (General Data Protection Regulation, L 119) and the

Law 4624/2019 (Government Gazette A' 137), which must be notified in accordance with article 33 of the said Regulation, informs the Personal Data Protection Authority without undue delay .

2. Where the supervisory authorities referred to in Articles 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine in accordance with point (i) of paragraph 2 of Article 58 of that Regulation, the National Cybersecurity Authority shall not impose an administrative fine in accordance with Article 26 for an infringement referred to in paragraph 1 of this Regulation which results from the same conduct that was the subject of the administrative fine in accordance with point (i) of paragraph 2 of Article 58 of Regulation (EU) 2016/679. The National Cybersecurity Authority may in such a case apply the enforcement measures referred to in points (a) to (h) of paragraph 4 and in paragraph 5 of Article 24 and in points (a) to (g) of paragraph 4 of Article 25 of this Regulation.

3. If the supervisory authority competent in accordance with Regulation (EU) 2016/679 is established in another Member State of the European Union, the National Cybersecurity Authority shall inform the Personal Data Protection Authority of the possible breach of the data referred to in paragraph 1.

Article 28
Mutual assistance
(Article 37 of Directive (EU) 2022/2555)

1. Where an entity provides services in more than one Member State or provides services in a

or more Member States of the European Union and its network and information systems are located in one or more other Member States, provided that one of the members is Greece, the National Cybersecurity Authority cooperates with the competent authorities of the other Member States concerned and mutual assistance is provided, as needed.

This cooperation implies, at least, that:

a) The National Cybersecurity Authority informs and consults with the competent authorities of the other interested Member States regarding the supervisory and enforcement measures taken,

b) the National Cybersecurity Authority may request another competent authority to take supervisory or enforcement measures and vice versa,

c) the National Cybersecurity Authority, upon receipt of a substantiated request from another competent authority, shall provide the other competent authority with mutual assistance commensurate with the resources available to it, so that the supervisory and enforcement measures can be implemented in an effective, efficient and consistent manner.

The mutual assistance referred to in point (c) may cover requests for information and supervisory measures, including requests to carry out on-site inspections or off- site supervision or targeted security checks. The National Cybersecurity Authority shall not refuse the request for assistance unless it is established that it is not competent to provide the requested assistance, that the requested assistance is not proportionate to its supervisory tasks or that the request concerns information or involves activities the disclosure or execution of which would be contrary to the essential interests of national security, public security or defence of Greece. Before refusing such a request, the National Cybersecurity Authority shall consult the other competent authorities concerned and, at the request of one of the Member States concerned, the European Commission and ENISA.

2. Where appropriate and by mutual agreement, the competent authorities of the Member States referred to in paragraph 1 may undertake joint supervisory actions.

Article 29
More specific regulations for providers of public or publicly available electronic communications networks electronic communications services

1. The Communications Privacy Authority (CPA) may, within the framework of its responsibilities, oblige providers of public electronic communications networks or publicly available electronic communications services to take enhanced cybersecurity measures, in addition to those provided for in the other provisions of this Part.

2. Providers of public electronic communications networks or publicly available electronic communications services shall notify, without delay, any circumstance that has a significant impact on the operation of the networks.

networks and services to ADAE in accordance with its regulations in force at any time and to the National Cybersecurity Authority (NACA) in accordance with article 16. NACA in turn notifies the events that have an impact on the availability or integrity of networks or services to the National Telecommunications and Post Commission. ADAE may inform the public or require such information from providers, provided that it considers that the disclosure of the event is in the public interest.

3. ADAE cooperates, as appropriate, in accordance with the provisions of applicable legislation, with the competent law enforcement authorities, with the Hellenic Data Protection Authority and with the Personal Data Protection Authority (HDPA).

4. The National Cybersecurity Authority (NSFP) is designated as a sectoral point of contact and cooperation at national level with the National Cybersecurity Authority (NSFP) with regard to providers of public electronic communications networks or publicly available electronic communications services, pursuant to the second paragraph of paragraph 6 of article 13. The joint ministerial decision of paragraph 26 of article 30 does not affect the responsibilities of the National Cybersecurity Authority or the NSFP, based on the applicable general or specific provisions of national, EU and international legislation.

CHAPTER EIGHT
AUTHORIZING, TRANSITIONAL, FINAL AND REPEATED PROVISIONS

Article 30
Authorizing provisions

1. By joint decision of the Ministers of Digital Governance and Interior, it is possible to postpone the entry into force of sub-paragraph fb) of paragraph f) of paragraph 2 of article 3.

2. a) By joint decision of the Minister of Digital Governance and the relevant Minister, which is issued after an opinion from the Director of the National Cybersecurity Authority, other public or private sector bodies may be included in the scope of application of this Article 3 and any specific issue for their inclusion may be determined.

b) By a similar decision, specific entities carrying out activities in the fields of national security, public order, defence or law enforcement, including activities related to the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 6 of Article 3, may be exempted from the scope of Article 3 from the obligations laid down in Articles 15 or 16, in respect of those activities or services. Where entities carry out activities or provide services exclusively of the type referred to in the first paragraph of this Article, they may be exempted from the obligations laid down in

articles 4 and 19 under the terms and conditions set out in the joint ministerial decision of the first paragraph hereof.

c) By decision of the Director of the National Cybersecurity Authority , the cases of paragraph 2 of article 3 may be specified .

3. By decision of the Director of the National Cybersecurity Authority , issued no later than four (4) months from the entry into force of this Regulation, the list of article 4 shall be drawn up for the basic and important entities as well as the entities providing domain name registration services, which shall be reviewed and, where appropriate, updated on a regular basis and at least every two (2) years.

4. By decision of the Minister of Digital Governance , a digital platform is created for the registration of basic and important entities, other methods of their registration are defined, the terms, procedure , details and the possibility of extending the registration deadline are determined, as well as the templates for submitting the data of paragraph 3 of article 4 and paragraphs 1 and 2 of article 19.

5. By a decision of the Minister of Digital Governance issued within six (6) months from the entry into force of this Act, following the opinion of the Director of the National Cybersecurity Authority, the National Cybersecurity Strategy of article 7 is approved. By a similar decision, the National Cybersecurity Strategy and the Action Plan for its implementation are updated, which constitutes an integral part thereof.

6. By decision of the Director of the National Cybersecurity Authority , which is issued within four (4) months from the entry into force of this Regulation, the capabilities, means, fixed assets, human resources and procedures that can be used in the event of a crisis pursuant to Article 9 are determined.

7. By decision of the Director of the National Cybersecurity Authority, which is issued within six (6) months from the entry into force of this and approved within an exclusive period of one (1) month by the Coordination Committee for Cybersecurity issues of article 23 of law 5002/2022 (Government Gazette A' 228), the national plan for responding to large- scale incidents and crises in cyberspace of paragraph 2 of article 9 of this is drawn up.

8. By decision of the Minister of Digital Governance and the relevant Minister, as the case may be, which is issued following the opinion of the Director of the National Cybersecurity Authority, other CSIRTs may be designated within the framework of article 10, if deemed necessary to achieve a high level of cybersecurity, taking into account the technical capabilities required for the performance of the relevant tasks .

9. By decision of the Director of the National Cybersecurity Authority , special response teams may be established to deal with incidents in the field of cybersecurity referred to in article 10. Special For the response to incidents in organizations referred to in paragraph f) of paragraph 2 of article 3, the response team is established by joint decision of the Director of the National Cybersecurity Authority and the Director of the National Intelligence Service.

10. By decision of the Director of the National Cybersecurity Authority, specific measures, procedures and means shall be taken to ensure the anonymity of persons reporting the vulnerability in accordance with paragraph 2 of article 12.

11. By decision of the Minister of Digital Governance and the relevant Minister supervising the respective body and, in the event of non-supervision, the highest administrative body of the relevant body, it is possible to designate authorities, bodies, services or organic units of the public administration with regulatory and supervisory responsibilities in individual sectors of Annexes I and II of this part, as sectoral points of contact and cooperation at national level with the National Cybersecurity Authority (National Sectorial Focal Points, NSFPs) in accordance with article 13.

This decision determines:

a) any specific issue related to the cooperation between the National Cybersecurity Authority and the NSFP, especially in the context of the mutual exchange of information , coordinated supervision, effective implementation, monitoring and feedback of the national strategic planning and the establishment of more specific cybersecurity measures for the relevant sector,

b) any specific issue related to the cooperation of the relevant services in matters of management and investigation of cybersecurity incidents, as well as crisis management.

12. By a joint decision of the Ministers of Digital Governance, Education, Religious Affairs and Sports and Labor and Social Security, which is issued after an opinion from the Director of the National Cybersecurity Authority, the procedures, the duration of training, the qualifications of the trainers, the educational material, the possibility of granting certification by the National Cybersecurity Authority and any other matter relevant to the implementation of paragraph 2 of article 14 are determined. By the same decision , the above training may be made mandatory for employees of the key and important entities that are competent, in accordance with their respective organizational charts or the relevant decisions assigning tasks for the cybersecurity of the said entities.

13.a. By decision of the Minister of Digital Governance, the national framework of cybersecurity requirements is determined, which includes the technical, operational and organizational measures for managing the cybersecurity risks of paragraph 2 of article 15, which are taken by the basic and important entities.

b. By decision of the Minister of Digital Governance , every necessary detail regarding

with the qualifications, duties, incompatibilities and obligations of the Information and Communications Systems Security Officers (ICSSOs) of paragraph 5 of article 15 for categories of entities that fall within the scope of this law.

14. By decision of the Director of the National Cybersecurity Authority, the standardized template is determined according to which the unified cybersecurity policy is prepared by the entities of the first subparagraph of paragraph 5 of article 15, which is evaluated and approved by the National Cybersecurity Authority .

15. By decision of the Director of the National Cybersecurity Authority, the details of the implementation of article 15 are regulated, and specifically:

a) any issue related to the preparation, evaluation and approval of the unified cybersecurity policy, more specifically issues related to the submission of a unified cybersecurity policy by significant entities, as well as the methodology and standards for recording and prioritizing tangible and intangible information and communication assets,

b) the suitability and specificity of the measures of the national framework of cybersecurity requirements in accordance with paragraph 2 of article 15 hereof, their technical and methodological requirements, taking into account the implementing acts issued by the European Commission in accordance with paragraph 5 of article 21 of Directive 2022/2555, based on the characteristics of the entities.

16. By decision of the Director of the National Cybersecurity Authority , the conditions and necessary details for the characterization of an incident as significant in accordance with article 16 may be specified, as well as the individual details for the procedure for reporting and managing security incidents, without prejudice to the relevant implementing acts of the European Commission.

17. By decision of the Director of the National Cybersecurity Authority, the provisions of paragraph 6 of article 15 may be carried out .

18. By joint decision of the Director of the National Cybersecurity Authority and the President of the National Telecommunications and Post Commission of article 6 of law 4070/2012 (Government Gazette A' 82), the terms and procedures for the publication of the policies and procedures of paragraph 3 of article 20 are determined. A similar decision may determine the terms and procedures for the publication of the necessary data, as well as any other matter relevant to the implementation of article 20.

19. By decision of the Director of the National Cybersecurity Authority, measures and actions are provided for the exchange of information in the field of cybersecurity referred to in paragraphs 1 and 2 of article 21, as well as supporting measures for the implementation of these regulations, in accordance with the policies referred to in paragraph h) of paragraph 2 of article 7. The above measures and actions may be specified in operational elements, including the use of specific information and communication technology (ICT) platforms and automation tools, the content and terms of the information exchange arrangements, taking into account any guidance issued by the European Union Agency for Cybersecurity (ENISA) pursuant to paragraph 5 of Article 29 of Directive 2022/2555. The same or similar decision shall determine the terms and details of the participation of the entities referred to in paragraph f) of Article 3, paragraph 2, in the arrangements of Article 21, on the exchange of information in the field of cybersecurity.

20. By a joint decision of the Ministers of National Economy and Finance and Digital Governance, which is issued after an opinion of the Director of the National Cybersecurity Authority within three (3) months from the entry into force of this Regulation, the amount, criteria and procedure for payment of the supervision fee and the audit fee of paragraph 1 of Article 23 are determined, any exceptions from their imposition, any issue related to the management and payment of the above fees and charges, as well as the amount of compensation for the bodies participating in the audit process, including certified inspectors and certified technical experts, in accordance with Article 23.

21. By decision of the Director of the National Cybersecurity Authority, control and inspection tasks are assigned, pursuant to article 23, to persons certified by the same Authority (“certified inspectors”), in accordance with the Control and Supervision Regulation of the National Cybersecurity Authority. By a similar decision, for the more effective exercise of the supervisory work of the National Cybersecurity Authority, it is possible to designate persons who meet the requirements of the Control and Supervision Regulation of the National Cybersecurity Authority as certified technical experts (Subject Matter Experts, SMEs) for the contribution of specialized expertise concerning information and communication systems and technologies.

22. By decision of the Governor of the National Cybersecurity Authority, which shall be issued within three (3) months from the entry into force of this Regulation, the Control and Supervision Regulation of the National Cybersecurity Authority of Article 23 is approved, which regulates the control and supervision methodology and the required procedures based on the risk-based approach, the bodies exercising control and supervision, the powers, incompatibilities and conflict of interest issues of these bodies, the qualifications of certified inspectors and certified technical experts, the periodicity of controls and on-site verifications of the unified cybersecurity policies of key and significant entities, in compliance with the principles of risk-based supervision, as well as any other matter related to Articles 24 and 25.

23. By a joint decision of the Ministers of National Economy and Finance, Interior and Digital Governance, which is issued following an opinion from the Director of the National Cybersecurity Authority, the terms, conditions and procedure for imposing the fines of article 26 are determined, taking into account at least the elements of par. 7 of article 24, the possibility of imposing periodic financial sanctions and the cases in which the amount of the fine may be adjusted, as well as the terms, conditions and procedure for collecting and paying the fines of article 26.

24. By decision of the Director of the National Cybersecurity Authority, the entities of article 4 that fall within the scope of sub-paragraph ab) of paragraph a) of paragraph 2 of article 31 of the
Law 5002/2022 (Gazette A' 228).

25. By the procedure of paragraph l) of paragraph 1 of article 6 of law 3115/2003 (A' 47), ADAE may adopt a Regulation for the implementation of paragraph 1 of article 29 hereof, applying, as appropriate , the sanctions of the Regulation and law 3115/2003.

26. Within four (4) months from the entry into force of this Act, by joint decision of the Ministers of Digital Governance and Justice, any specific issue relevant to the cooperation between the N.A.K. and the A.D.A.E. as NSFP shall be determined, in particular in the context of the mutual exchange of information, coordinated supervision, effective implementation, monitoring and feedback of the national strategic planning and the establishment of more specific cybersecurity measures for the relevant sector, any specific issue relating to the cooperation of the relevant services in matters of management and investigation of cybersecurity incidents, significant incidents , as well as crisis management.

Article 31
Transitional and final provisions

1. Until the issuance of the certificate of the Director of the National Cybersecurity Authority on the adequacy of the means and resources of the Computer Security Incident Response Team (CSIRT) of the National Cybersecurity Authority, the organizational unit of the General Staff of National Defense responsible for cyber defense issues is designated as the Computer Security Incident Response Team (CSIRT) and supports the CSIRT of the National Cybersecurity Authority in the performance of the tasks of paragraph 1 of article 10.

2. Where in the applicable legislation:

a. reference is made to Law 4577/2018 (A' 199) on issues related to the security of network and information systems, this law is understood,

b. reference is made to bodies falling within the scope of application of Law 4577/2018 or to the operators of essential services of paragraph 4 of Article 3 of the Law 4577/2018 or the digital service providers of paragraph 6 of article 3 of Law 4577/2018, means the basic entities of paragraph 1 of article 4 of this law.

3.a. Until the issuance of the decisions of paragraph a) of paragraph 13 and paragraph b) of paragraph 15 of article 30 and in any case no later than six (6) months from the publication of this, the Regulation on the Security of Electronic Communications Networks and Services (no. 28/2024 decision of the Communications Privacy Authority, B' 551) shall apply, to the extent that it concerns the issues of this Part regarding the obligations of providers of public electronic communications networks or publicly available electronic communications services.

b. Until the issuance of the decision of paragraph 25 of article 30 and in any case no later than six (6) months from the publication of this, the Regulation on the Security of Electronic Communications Networks and Services (decision no. 28/2024 of the Authority for the Protection of Communications Privacy) shall apply, to the extent that it concerns the enhanced cybersecurity measures of paragraph 1 of article 29.

Article 32
Repealed provisions

From the entry into force of this Part, the following are repealed:

a) articles 148, on security of networks and services, and 149, on implementation and enforcement, of the
Law 4727/2020 (Government Gazette 184) and

b) articles 1 to 16 of Law 4577/2018 (Government Gazette A' 199), on the incorporation into Greek legislation of Directive 2016/1148/EU of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union and the decision no. 1027/4.10.2019 of the Minister of State "Issues of implementation and procedures of Law 4577/2018 (Government Gazette A' 199)" (Government Gazette B' 3739).

PART B
NATIONAL AUTHORITY PERSONNEL ARRANGEMENTS
CYBERSECURITY AND OTHER PROVISIONS

Article 33
National Authority personnel arrangements
Cybersecurity - Amendment
article 21 of law 5086/2024

In paragraph 4 of article 21 of law 5086/2024, on the transitional provisions of Part A of this law, the following amendments are made: a) in the first paragraph, the date "December 31, 2024" is replaced by the date "December 31, 2025", b) in the second paragraph, the date "January 1, 2025" is replaced by the date "January 1, 2026" and paragraph 4 is worded as follows:

"4. Until December 31, 2025, the total cost of payroll, as well as any type of remuneration, including the salary difference resulting from the implementation of this provision, shall be borne by the budget of the Ministry of Digital Governance and shall be paid by it. Without prejudice to paragraph b)

of paragraph 3 of article 13, from January 1, 2026, the total cost of payroll, as well as any type of remuneration, shall be borne by the Authority and paid by it."

Article 34
Arrangements for the appointment of an Information and Communications Systems Security Officer - Amendment to paragraph 1 of article 18 of Law 4961/2022

1. In paragraph 1 of article 18 of law 4961/2022 (Government Gazette A' 146), on the Information and Communications Systems Security Officer, the following amendments are made: a) in the first paragraph, the words "IT or IT TE" are replaced by the words " IT IT sector PE of any specialty or IT TE category of IT sector IT specialty (SOFTWARE or HARDWARE)", b) a new, second, paragraph is added and paragraph 1 is worded as follows:

"1. In each central government body within the meaning of paragraph c of paragraph 1 of article 14 of Law 4270/2014 (Government Gazette A' 143), one (1) employee of the IT sector category PE of any specialty or the IT sector category TE of the IT sector specialty (SOFTWARE or HARDWARE) shall be appointed as the IT and Communications Systems Security Officer (YASPE) with his deputy. In the absence of an employee of the IT or IT sector category PE , an employee of any IT or TE category shall be appointed by the decision of the first paragraph . The YASPE shall be appointed based on the experience he has in the field of cybersecurity."

2. In paragraph 4 of article 113 of law 4961/2022, on authorizing provisions, paragraph e) is added, as follows:
"e) By joint decision of the Minister of Digital Governance and the relevant Minister, issued upon a recommendation from the national cybersecurity certification authority referred to in paragraph 1 of Article 15, national cybersecurity certification schemes for ICT products, services and procedures may be established, applying the requirements of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA ("European Union Agency for Cybersecurity") and on cybersecurity certification in the field of information and communications technology and repealing Regulation (EU) 526/2013 (Cybersecurity Act) (L 151)."

Article 35
Settings for areas outside television coverage

1. The Ministry of Digital Governance may finance all costs for the supply , installation, operation, upgrade and maintenance of Supplementary Coverage Stations (S.S.K.), including the cost of licensing the construction of antennas, which are installed for the purpose of to serve the television coverage needs of the local population in areas of the Greek territory that do not have satisfactory access to a terrestrial digital broadcasting signal, in accordance with the applicable provisions on state aid. The above expenses are covered within the framework of relevant actions, by the Public Investment Program.

2. The determination of the areas, as well as the optimal method and sequence of their coverage, is carried out following a study by the General Secretariat of Telecommunications and Posts (GSPT) of the Ministry of Digital Governance, which assumes the role of the central coordination body for the implementation of the individual actions.

3. Upon request of the General Secretariat of the Hellenic Republic, the National Network of Technology and Research Infrastructures (EDYTE S.A.) may undertake, as implementing body, the awarding process, preparation, administration and management of the necessary contracts for the implementation of the said actions.

4. The responsible party for the installation, commissioning , use and maintenance of the Supplementary Coverage Stations is the selected digital terrestrial broadcasting network provider , which has been awarded the rights to use the radio frequencies used by the S.S.K. in accordance with the provisions of the applicable legislation.

5. The joint decision under reference ÿÿÿ.14177 EX/ 14.5.2021 of the Ministers of Development and Investment, Interior , Digital Governance, State and the Deputy Minister to the Prime Minister (B' 2066), on ensuring access of permanent residents of Areas Outside Television Coverage to the programs of Greek free-to-air television stations with national coverage , is repealed upon publication of this.

Article 36
New deadline for correcting first registrations - Possibility of correcting first registrations in areas where the possibility of challenging an inaccurate registration with the indication "unknown owner" had expired - Amendment to article 102 Law 4623/2019

1. In paragraph 2 of article 102 of law 4623/2019 (A' 134), on regulations of the Ministry of Environment and Energy, the following amendments are made: a) in the first paragraph, the words "on 30.11.2024" are replaced by the words "after the lapse of one (1) year from the publication of an act of the Board of Directors of the Public Legal Entity "Hellenic Land Registry" which establishes the implementation of the Land Registry system in replacement of the system of transfers and mortgages throughout the territory of the country", b) in the second paragraph the date "31.12.2015" is replaced by the date "31.12.2017" and paragraph 2 of article 102 is worded as follows:

"2. For the areas declared under cadastral registration before the entry into force of Law 3481/2006

(A' 162), the exclusive deadline of paragraph a' of paragraph 2 of article 6 of law 2664/1998, if it or its extensions had not expired by 30.11.2018, expires after the lapse of one (1) year from the publication of an act of the Board of Directors of the Public Legal Entity "Hellenic Land Registry " which establishes the application of the Land Registry system in replacement of the system of transfers and mortgages throughout the territory of the country. The above deadline also applies to the areas in which the first entries were registered from 1.1.2013 to 31.12.2017. Exceptionally, for the areas that were declared under cadastral registration before the entry into force of law. 3481/2006 (A' 162), at the entry into force of Law 4623/2019 (A' 134) were still under cadastral registration and the declaratory act of completion of the cadastral registration and the decision to enter into force of the Cadastre had not been issued, the exclusive deadline of paragraph a of paragraph 2 of article 6 of

Law 2664/1998 expires on December 31 of the year in which eight (8) years have passed since the date of entry into force of the Land Registry."

2. In paragraph 2A of article 102 of law 4623/2019, the following amendments are made: a) in the first paragraph , the date “30.11.2024” is replaced by the words “one (1) year from the publication of an act of the Board of Directors of the Public Legal Entity “Hellenic Land Registry” establishing the application of the Land Registry system in replacement of the system of transfers and mortgages throughout the territory of the country”, b) in the fourth paragraph, the date “30.11.2024” is replaced by the words “one (1) year from the publication of an act of the Board of Directors of the Public Legal Entity “Hellenic Land Registry” establishing the application of the Land Registry system in replacement of the system of transfers and mortgages throughout the territory of the country”. "Hellenic Land Registry" which establishes the application of the Land Registry system in replacement of the system of transfers and mortgages throughout the territory of the country:" and paragraph 2A of article 102 is formulated as follows:

"2A. For the areas in which the exclusive deadline of paragraph a' of paragraph 2 of article 6 of law 2664/1998, on the correction of first registrations, had expired by 30.11.2018, the possibility of challenging and correcting an inaccurate registration, on real estate with the indication "unknown owner", either out of court, when the conditions of sub-paragraphs aa), ab), ag) and ad) of paragraph b) of paragraph 1 of article 18 of law 2664/1998 are met, or following the filing of a lawsuit in accordance with paragraph 2 of article 6 of the same law, is possible until the lapse of one (1) year from the publication of an act of the Board of Directors of the Public Legal Entity. "Hellenic Land Registry" which establishes the application of the Land Registry system in replacement of the system of transfers and mortgages throughout the territory of the country, only if, after the expiry of the exclusive deadline for each region, no subsequent acts have been registered on the cadastral sheet of the property. Registration of the action of par. 2 of article 7 of law 2664/1998 is not taken into account as subsequent ster act. In any case, the plaintiff may waive the action of the previous paragraph and follow the other correction procedures or persist in his/her filed action. For the areas of the first paragraph of this article, it is permitted, until the lapse of one (1) year from the publication of an act of the Board of Directors of the Public Legal Entity "Hellenic Land Registry", which establishes the application of the Land Registry system in replacement of the system of transfers and mortgages throughout the territory of the country: a) the correction of an inaccurate registration with the indication "Greek State", in accordance with the procedure of par. 4 of article 6 of the law. 2664/1998, when the title of the person requesting the correction or of his licensors (direct or remote) is a concession of the Greek State and b) the correction of the inaccurate registration by the procedure of par. 4 of article 6 when in the relevant cadastral sheets, during the finalization of the initial registrations, the licensor of the person requesting the correction was recognized as the beneficiary of the right , while the title of acquisition of the relevant right by the person requesting the correction is transcribed in the transcription books of the corresponding Mortgage Registry or Cadastral Office and under the condition that no other, incompatible in content, registration has occurred in the cadastral sheet in the meantime.

Article 37
Arrangements for supporting the information systems of health units of the National Health System

The contract no. 2/30.1.2024 of the non-profit limited liability company with the name "ELECTRONIC GOVERNANCE OF SOCIAL SECURITY S.A." and the distinctive title "H.I.D.I.K.A. S.A." with the subject "Unified Information System to support the operational operations of the health units of the National Health System (EPSMY) of H.I.D.I.K.A. S.A.", Subproject 3 "Provision of development services and production operation of H.I.D.I.K.A. S.A. in the health sector" is automatically extended from its expiration until 29.4.2025. The contract terminates automatically and before the end of the deadline of the above paragraph, with the signing of a contract of the same subject matter within the framework of the new tender procedure carried out by H.D.I.K.A. S.A.

Article 38
Local call for temporary recruitment substitute teachers - Add article 63A in law 4589/2019

After article 63 of law 4589/2019 (A' 13), article 63A is added, as follows:

"Article 63A
Local call for the recruitment of temporary substitute teachers

1. Teachers may be hired as temporary substitutes, full-time or part-time.

rium, with a fixed- term private law employment relationship and with a maximum duration until the end of the academic year, after the issuance of the invitation to express interest in par. 2, provided that: a) the procedure of article 86 of law 4547/2018 (A' 102) has been followed and b) there are operational needs for teaching positions in primary and secondary education school units in specific areas of the country, which cannot be covered by the ranking lists of the Supreme Personnel Selection Council (ASEP) due to the exhaustion of candidates.

2. By means of an invitation to express interest issued by the Regional Director of Education, following an opinion from the Director of Education, which is posted in the Diavgeia program and on the websites of the Ministry of Education, Religious Affairs and Sports , the Regional Directorate of Education and the Directorate of Education, candidates are invited to submit an application to school units in the areas of appointment under the responsibility of the relevant Directorate of Education . The local invitation specifies the advertised positions of par. 1 per school unit, per sector/ specialty, the hours of employment, the recruitment procedure and the exclusive deadline for submitting the application.

3. Candidates who possess the formal qualifications for entry and appointment in the relevant sector may participate in the application process .
specialty and are not included in the current ranking lists of the A.S.E.P.. Candidates are ranked in selection lists by branch/ specialty based solely on the grade of their degree. In the event of equality of degrees, candidates with the oldest degree take precedence according to the date of its award. In the event that the degrees have been awarded on the same date, then the ranking is based on the seniority of the candidates' registration in the Integrated Information System for Primary and Secondary Education Personnel Management (OPSYD). In particular , primary and secondary education teacher candidates with specialization in Special Education (SEE) are ranked in the selection evaluation tables based only on the grade of their basic degree, but in the event of equality of degrees, candidates with the oldest special formal qualification for inclusion in the SEE branch take precedence. For kindergarten teachers and SEE teachers, the ranking is carried out uniformly for candidates in the branches PE61 and PE60 with specialization in SEE and PE 71 and PE 70 with specialization in SEE, respectively. Otherwise, paragraph d) of paragraph 4 of article 58 applies. The application serves as a solemn declaration of article 8 of

Law 1599/1986 (A'75) for the information contained therein. The selection evaluation tables are valid until the end of the academic year. When submitting applications, candidates confirm that they do not fall under in par. 5A of article 62, on the exclusion of teachers and members of the Special Educational Service or Special Educational Service who have been appointed or are being appointed by a new appointment or recruitment for three (3) years, and in par. 5A of article 63, on the exclusion of teachers and members of the Special Educational Service or Special Educational Service who are hired as substitutes and refuse to take up service or resign, during the year of recruitment and the following school year, of this Act, as well as in par. 4 of article 86 of law 4547/2018, on the exclusion of teachers and members of the Special Educational Service or Special Educational Service who are hired as substitutes following a special invitation and refuse to take up service or resign, during the year of recruitment and the following school year.

4. The selection evaluation tables of par. 3 are prepared under the responsibility of the relevant Director of Education, are ratified by the Regional Director of Education and are posted on the websites of the Ministry of Education, Religious Affairs and Sports, the Regional Directorate of Education and the Directorate of Education.

A reform of the lists, which entails a reclassification of the candidates, is carried out by the relevant Director of Education and those not entitled to be hired based on the new classification are dismissed. Those dismissed receive the salaries provided for their employment up to the date of dismissal , without any compensation for this reason.

5. If the operational needs for teacher positions under paragraph 1 are not met and after the call for expressions of interest under paragraph 2, it is possible to recruit retired teachers who have not exceeded the age of sixty-seven (67), in accordance with the provisions herein.

6. The recruitment of teachers is carried out by the relevant Director of Education, according to the number of functional vacancies to be filled per sector/specialty, educational structure and level of education, which have been approved by a relevant act of the Minister of Education, Religious Affairs and Sports and regardless of the source of funding immediately after the posting of the candidate selection evaluation tables in accordance with par. 3.

7. When additional operational needs arise for positions in a school unit and discipline/specialty that was included in the local call for expressions of interest in paragraph 2, those registered on the selection evaluation lists in paragraph 3, who have not already been hired, may be invited, throughout the academic year, to express interest in hiring.

8. The previous service acquired through the present procedure is not counted in the priority ranking procedure announced and carried out by the A.S.E.P. in application of the provisions in force each time, but is considered as actual public educational service and is taken into account after the permanent appointment in public education for any consequence."

Article 39
Textbooks - Register of Textbooks - Digital Library of Textbooks - Amendment of par. 5, 6, 7, 17 and 20 and addition of par. 23 and 24 to article 84 of Law 4823/2021

1. In par. 5 of article 84 of law 4823/2021 (A' 136), on the writing of textbooks - textbook register and digital library of textbooks , the last paragraph is deleted, and par. 5 is worded as follows:

"5. For the writing of the textbooks of par. 1 for inclusion in the M.D.B. and the P.B.D.B., an invitation for expressions of interest is issued by the Minister of Education, Religious Affairs and Sports, following a recommendation by the I.E.P., which is posted on the website of the Ministry of Education, Religious Affairs and Sports, the I.E.P., the I.T.Y.E. "DIOFANTOS" and the Greek Book Association and which specifically mentions the specifications and characteristics of the books, the scientific and pedagogical conditions for inclusion, the timetable and the procedure for submitting applications and deliverables by interested parties. The specifications and technical characteristics concerning the printing or digital version of the delivered books are recommended by the I.T.Y.E. "DIOPHANTUS"

2. Paragraph 6 of article 84 of Law 4823/2021, on the evaluation of textbooks, is replaced as follows:

"6. Following completion of the public call for interest process and approval of the participation applications, participants upload to the digital book submission system of FORTH "DIOFANTOS ": a) the textbook in all the provided digital formats, b) the digital supplementary material (learning objects), c) the digital pre-print material and d) the metadata of all necessary elements. The evaluation of submitted textbooks is carried out by scientific committees, established per subject, in two (2) stages of control: a) completeness, where proposals containing obvious errors and deficiencies are rejected, and b) quality, with criteria determined based on specifications and characteristics of scientific and pedagogical suitability, in order to enable the assessment, in particular, of the scientific , pedagogical and didactic validity of the book and other educational material, the encouragement of student initiative and aesthetic taste, as well as specifications related to the technical characteristics of the books, such as dimensions, visual material and standardization parameters . During the evaluation stage of the submitted textbooks, the evaluation committee may set exclusive deadlines for participants to complete, specify or send any necessary clarifications, the failure to do so will lead to their rejection."

3. In paragraph 7 of article 84 of Law 4823/2021 on textbook evaluation committees, the following amendments are made: a) in the first paragraph, the word "consist" is replaced by the word "are assembled" and b) in the second paragraph, after the words "in the control" the words "completeness and quality of paragraph 6, with control" are added and paragraph 7 is worded as follows:

"7. The scientific committees of par. 6 are formed by members of the faculty, teachers and other scientists with advanced qualifications and knowledge in the scientific and pedagogical subject of the books. The work of these committees is assisted by experts, with regard to the completeness and quality control of par. 6, by checking compliance with the specifications and technical characteristics relating to the printing or digital version of the books to be delivered. The members of the scientific committees and the experts are not related to the writing process of the books under inclusion. The formation of the scientific committees and the selection of the experts is carried out by the Board of Directors (BoD) of the IEP, upon its invitation. For the evaluation of the experts, the committees also include executives of the I.T.Y.E. "DIOPHANTOS". The term of office of the members of the scientific committees ends after the ministerial decisions to include the books in the M.D.B. and P.B.D.B. become final and irrevocable."

4. Paragraph 17 of article 84 of Law 4823/2021, on the procedure for writing textbooks, is replaced as follows:

"17. If the process of writing textbooks and their inclusion in the M.D.B. and the P.B.D.B. proves fruitless or there are not at least two approved applications for participation per course or, during the stage of completeness evaluation in accordance with the second paragraph of par. 6, the remaining proposals for scientific evaluation fall short of two (2), or it concerns the inclusion of textbooks in the M.D.B. and in the PSB, which correspond to subjects of vocational education and special education, by decision of the Minister of Education, Religious Affairs and Sports, following a recommendation from the IEP, it is possible, alternatively, even before the completion of a previous call for expressions of interest: a) the partial repetition of the call for expressions of interest to cover the remaining subjects, b) the issuance of a new, full or partial, call for expressions of interest, in order to have at least two (2) textbooks per subject, with similar or different terms from the previous call, c) the assignment of the writing to groups of teachers, consisting of teachers serving in the IEP or seconded to the IEP. for this writing or by other scientists with increased qualifications and knowledge or d) the assignment of the writing, in compliance with the provisions of

Law 4412/2016 (A' 147), to natural or legal persons or the

conclusion of programmatic agreements for this purpose, between the IEP and the AEI. Special provisions for the textbooks of vocational education and special education and training remain in force.

5. In par. 20 of article 84 of law 4823/2021, on textbooks - textbook register - digital textbook library, the following amendments are made: a) the words “according to their competence” are deleted, b) after the word “criteria” the words “of textbooks ” are added, c) after the second mention of the words “more specific conditions”, the words “the submission and examination procedure, as well as the control bodies” are replaced by the words “submission of an expression of interest and an application to participate in the calls for interest of par. 5, the procedure for submitting and evaluating textbooks, as well as the evaluation bodies”, d) the words “of the call for expressions of interest of par. 5 and” are deleted and, following legislative improvements, par. 20 is formed as follows

"20. By decision of the Minister of Education, Religious Affairs and Sports, issued following recommendations from the IEP and the ITYE "DIOFANTOS", the procedures for the creation, establishment, operation and technical support of the MDB and the PSDB are determined, the more specific conditions, specifications, characteristics and criteria of the textbooks, as well as the procedure for inclusion, modification, change and de-inclusion of textbooks in the MDB and the PSDB, the more specific conditions for submitting an expression of interest and an application for participation in the calls for interest as well as the content of the calls for interest referred to in par. 5, the procedure for submitting and evaluating textbooks, as well as the bodies for evaluating administrative appeals against decisions on inclusion, exclusion and determination of the reference price, the content of the agreements of par. 9, the more specific structure and organization of the M.D.B. and the P.B.D.B., the data registered in the M.D.B. for each specific book, as well as any other more specific issue concerning the implementation of this article.”

6. In article 84 of Law 4823/2021 on textbooks - textbook register - digital textbook library, paragraphs 23 and 24 are added as follows:

"23. By decision of the Minister of Education, Religious Affairs and Sports, following the recommendations of the IEP and the ITYE "DIOFANTOS", every issue related to the mode of operation and the scope of the scientific committees of par. 6 and the groups of par. c) of par. 17 is regulated. By a similar decision, every necessary detail for the commencement of the implementation of this, the procedure and the conditions for the use of the textbooks that have been included in the M.D.B. and P.V.D.B. is determined.

24. Approved bodies that participated in the event invitation under reference 46978/ÿÿ4/25.4.2023 of interest of the Minister of Education, Religious Affairs and Sports, who have posted all or part of the assessed material on the I.T.Y.E. “DIOFANTOS” platform within the deadline, but its final submission was not completed for any reason, may, within ten (10) days from the publication of this, definitively post the material, with the only condition being the presentation of a certificate from I.T.Y.E. “DIOFANTOS” certifying the submission of part or all of the material on the relevant I.T.Y.E. “DIOFANTOS” platform before the expiry of the final deadline for posting the assessed material. If the above approved participants have uploaded the necessary material on the relevant platform within the deadline, but this does not correspond to the total evaluated material of the textbooks, in relation to that included in their approved application for participation, they may, within ten (10) days from the publication of this and without further formality, submit their remaining material. If the above approved participants have uploaded incorrect material within the deadline, but by mistake, or material that requires necessary corrections or improvements, they may, within ten (10) days from the publication of this and without further formality, re-submit the material with the necessary corrections. The last paragraph of par. 6 also applies to proposals submitted in accordance with this.

Article 40
Maximum fee limit for doctors of the Special Body of Doctors of the Disability Certification Center - Amendment to paragraphs 3 and 4 of article 104 of Law 4961/2022

1. In the third paragraph of paragraph 3 of article 104 of the Law 4961/2022 (Government Gazette 146), on the health committees of the Disability Certification Center of the Electronic National Social Security Institution, the words "The Public Health Care Structures (D.D.F.Y.) and the National Organization for the Provision of Health Services (E.O.P.Y.Y.)" are replaced by the words "The Public Bodies", and par. 3 is worded as follows:

“3. The health committees are established by specialty and meeting based on the submitted requests for an opinion and the main diseases in them, the location of the doctor, the residence of the applicant, the available specialties and the minor age of the applicant . In the case of an examination of a minor, the committee includes a doctor from the National Institute of Health with a specialty in pediatrics or another pediatric specialty, if available. Public bodies must allow the doctors who serve them to participate in health committee meetings, to which they have been appointed, at least five (5) days per month. The decision appointing the health committee also appoints its chairman, who must hold a specialty corresponding to that of the committee.”

2. In par. 4 of article 104 of law 4961/2022, regarding the compensation paid by the Electronic

of the National Social Security Institution to the doctors of the Special Body of Doctors, who participate in the meetings of the committees of the Disability Certification Center, the following amendments are made : a) in the second paragraph the words “To the doctors” are replaced by the words “To the members”, b) at the beginning of the third paragraph the phrase “The evaluation requests are equally distributed among the doctors of the National Social Security Institution by category and specialty and”, c) in the third paragraph : ca) the words “From November 1, 2024” are added and cb) the word “double” is replaced by the word “triple”, d) a new fifth paragraph is added and following legislative improvements, par. 4 is worded as follows:

"4. The doctors of the National Health Insurance Corporation and the secretaries of the health committees of the National Health Insurance Corporation are paid by the e-EFKA compensation per assessed request, for which a final GA is issued. The members and secretaries of the Sampling Control Committee are paid by the e-EFKA compensation per audited incident. The evaluation requests are equally distributed among the doctors of the National Health Insurance Corporation by category and specialty and the compensation hereunder is paid in accordance with the joint decision of par. 5 of article 109. From November 1, 2024, the total amount of compensation cannot exceed three times the monthly maximum salary limit per year , as defined in par. 1 of article 28 of the law. 4354/2015 (A' 176). Exceptionally, the total amount of compensation per year may amount to five times the monthly maximum salary limit, as defined in par. 1 of article 28 of

Law 4354/2015, since the number of available, in accordance with the Regulation of Operation of the National Health Insurance Fund, doctors of the National Health Insurance Fund with a specialization in rheumatology, neurology and psychiatry, is not sufficient for the timely evaluation of pending applications. The travel expenses (travel expenses, overnight expenses, daily allowance) of the doctors of the National Health Insurance Fund who travel outside the headquarters to perform their duties as president or member of the health committees of the National Health Insurance Fund are paid by the e-EFKA , which are paid according to the provisions in force to the public servants who travel outside the headquarters. The maximum annual travel limit is set at ninety (90) days.

Article 41
Regulation of the urban transport project of the Regional Unit of Thessaloniki - Amendment of article 3, par. 4 of article 11 and par. 1 of article 26 of Law 4482/2017

1. In paragraph 1 of article 3 of law 4482/2017 (A' 102), on the responsibilities of the " Thessaloniki Transport Project Organization, Societe Anonyme", paragraphs l' to l'b' are added as follows:

"l. Promotes sales of fare products through the implementation of the discount policy.

Sells fare products and collects fares on behalf of transportation service providers .

of the Regional Unit of Thessaloniki of article 2, controls and returns the total revenue from sales of products of providers of the above transport projects to the state budget, following previous , in order, aa) deduction for return of the amount of Value Added Tax (VAT) due for the transport service, in accordance with the VAT legislation for the total amount of sales of fare products, b) withholding of the percentages determined in favor of it in accordance with article 11 on the total revenue from sales of fare products (excluding VAT), c) return to OASTH. of the remaining amount of sales of fare products for the provision of a transport project by i) the providers of public passenger urban transport by buses , with whom OSETH has a contract and ii) OASTH in accordance with paragraph 1 of article 26, in accordance with the invoiced service according to the applicable provisions. It may assign part of the responsibilities of this case to transport project bodies .

"lt. Controls, supervises, acts for and coordinates the interoperability of the transport project carried out by the providers of the public transport system, being able to contract with providers of the said transport project and third parties for the purpose of interoperability ."

2. In paragraph 2 of article 3 of law 4482/2017, paragraphs c' and d' are added, as follows:

"c. By joint decision of the Ministers of National Economy and Finance and Infrastructure and Transport, the procedure for the collection by OSETH S.A. of revenues for fare products sold on behalf of transport project providers of the Regional Unit of Thessaloniki of article 2, the amount or percentage of revenues from fares of transport project providers in accordance with paragraphs l' and la' of par. 1, the procedure and periodicity of the payment of the above amounts due by OSETH S.A. to OSETH and the state budget, as well as any other matter relevant to the implementation of paragraphs l' and la' of par. 1, are determined.

d. By decision of its Board of Directors, after the approval of the competent body of the Ministry of Infrastructure and Transport, OSETH selects the legal entity to which it assigns its responsibilities, in accordance with the last paragraph of the article.
of paragraph 1 of article 3."

3. In paragraph 4 of article 11 of law 4482/2017, a final paragraph is added and paragraph 4 is worded as follows:

"4. Specifically for O.A.S.T.H., the percentage of par. 1 is valid until June 30, 2020. From July 1, 2020, the above percentage is set at one point two percent (1.2%) of the total revenue derived from the provision of transportation services and the production of transportation work in the area of responsibility of O.A.S.T.H.. From December 1, 2024, the percentage of the second paragraph of this paragraph applies only

for the products of the price whose sales document is issued to the tax registration number of the OASTH, otherwise the percentage of par. 1 applies."

4. In the first paragraph of paragraph 1 of article 26 of the Law 4482/2017, the date "31.12.2024" is replaced by the date "31.12.2025", and par. 1 is amended as follows:

"1. The transport project in the Regional Unit of Thessaloniki is temporarily assigned to OASTH for the absolutely necessary time and in any case not after 31.12.2025. During the period of the temporary assignment of the transport project to OASTH, in accordance with the previous paragraph, the transport project will be provided under the same terms as the financial agreement of 30.4.2001 between the Greek State and OASTH, as it was in force after its amendment and supplementation on the date of publication of Law 4482/2017 and at the same time, the conclusion of the contracts provided for in the provisions of Article 54, paragraphs 3 and 4 of Law 4568/2018 is permitted for this transport project."

Article 42
Guides for the execution of the transportation project of the Thessaloniki Urban Transport Organization

1. Private Law Fixed-Term Employment Contracts for personnel, one hundred and fifty (150) drivers, specializing in Driver Training, who were hired by the private law legal entity, under the name "THESSALONIKI URBAN TRANSPORT ORGANIZATION"

"KIS" (O.A.S.T.H.), by virtue of the Announcement under the elements of SOX 1/2023, which were renewed with article 41 of Law 5131/2024 (A' 128) and have not been terminated by the time of publication of this, are automatically renewed from their expiration until the completion of the assignment of the transportation project to OASTH and in any case not later than June 30, 2025.

2. Private Law Fixed- Term Employment Contracts of forty (40) drivers, specializing in Driver Training, who were hired by OASTH, pursuant to the Announcement under reference SOX 1/2024 and have not been terminated by the publication of this, are automatically renewed from their expiration until the completion of the assignment of the transportation project to OASTH and in any case not beyond June 30, 2025.

3. The renewals of paragraphs 1 and 2 do not change the nature of the employment relationship, on the basis of which the employees were hired in these positions and are not counted towards the maximum period of twenty-four (24) months, within the meaning of articles 5 to 7 of Presidential Decree 164/2004 (Government Gazette A' 134).

Article 43
Urban railway licensing

1.a) For the commercial operation of an urban railway network or its extensions, an operating permit for the infrastructure and systems is granted.

this, under the responsibility of the competent Directorate of Fixed-Track Infrastructure, Maintenance and Safety (D14) of the Ministry of Infrastructure and Transport, following a proposal by HELLENIC METRO S.A.

b) For the granting of the permit referred to in paragraph a), the following are required:

ba) certificate of commencement of activity and tax registration number for HELLENIC METRO S.A.,

bb) building permit for the project,

bg) construction contractor certificate certifying that the works on the urban railway system under licensing have been completed and that all system performance tests have been completed,

bd) certificate from HELLENIC METRO S.A. for the integrity, safety, functionality and reliability of the project systems within the framework of its responsibilities as contracting authority,

be) a certificate from an independent certification body for the operation of the urban railway network,

bf) general overview of the project,

bg) declarations of conformity for lifts, accompanied by the certificates issued by a notified body, as appropriate, in the context of the conformity assessment procedure, as well as a certificate of registration of the lifts by the competent service of the relevant Municipality,

b) certificates of correct installation and operation (initial inspection) of type A' escalators and walkways, from a recognized inspection body for this purpose and

b) active fire protection certificate in accordance with article 8 of Fire Ordinance No. 13/2021 "Approval of Fire Ordinance No. 13/2021 on the subject: "Specification of the procedure for submitting the required supporting documents, checking and issuing administrative fire protection acts to enterprises - facilities, pursuant to article 167 of Law 4662/2020" (B' 5519)."

2. For the provision of passenger transport services via an urban railway network, with the assumption of the operation and maintenance of this network by a public or private public service provider , a service provision permit is granted, under the supervision of the competent Passenger Transport Directorate (D32) of the Ministry of Infrastructure and Transport, following an application by HELLENIC METRO S.A.

For the granting of the permit referred to in the first paragraph, the following are required:

a) a certificate from an independent certification body for the operation of the urban railway,

b) solemn declaration of undertaking the operation of the project ,

c) certificate of commencement of activity and tax registration number for the operating company and

d) certificate of incorporation of the operating company.

3. The scope of application of this Regulation excludes the railway project and facilities provided by the Hellenic Railways Organization, its subsidiaries , its affiliated companies, and the companies

infrastructure and exploitation of the railway network and any other public or private body with a similar purpose.

Article 44
Financial statements and activity reports of construction companies

For the year 2024, the deadline for submitting the annual financial statements and the activity report of the contracting companies of the first paragraph of par. 7 of article 41 of Presidential Decree 71/2019 (A' 112), on the maintenance of the Register of Public Works Contracting Companies (MH.EEDE) and MH.EEDE certificates, to the Registers Directorate of the General Secretariat of the

The Infrastructure Fund of the Ministry of Infrastructure and Transport is extended from its expiry date until 19.2.2025.

PART C
ENTRY INTO FORCE

Article 45
Entry into force

1. Without prejudice to paragraph 2, the force of this law shall commence upon its publication in the Government Gazette.

2. The validity of sub-paragraph fb) of paragraph f) of paragraph 2 of article 3 begins one (1) year from the publication of this in the Government Gazette.

I

(() 2022/2555)

1.	)	, . 3 . () . 2 4001/2011 (' 179), "", . 1 . () . 2 4001/2011.
		, . 1 . () . 2 4001/2011.
		, . 3 . () . 2 4001/2011.
		. , () . 3 2 .4001/2011.

		, . 8) 2 () 2019/943 5 2019, (L 158). — , . 25) 2 () 2019/943, , , . (), () () . 3 2 . 4001/2011 — , , .
	)	, . . 32 2 . 3468/2006 (' 129).
	)	.
		, , .
		, ' . 2 2 . 4123/2013 (' 43).

	)	, . () . . 2 2 4001/2011.
		. () . . 1 2 4001/2011.
		, . . 2 2 (1) . 4001/2011.
		, . . 2 2 () . 4001/2011.
		, . () . . 2 2 4001/2011.
		, . () . . 2 2 4001/2011.
	)	,
2.	)	, . 3 4) () 300/2008, .

		, ' . . 1 2 .. 52/2012 (' 102), , . ' . 1 2 .. 52/2012, 2 K () 1315/2013 11 2013, A 661/2010/EU (L 348), .
		, , . 1 2 K () 549/2004 10 2004, («- ") (L 96).
	)	, . 2) 3 . 4408/2016 (135).
		, . 1) 3 . 4408/2016, , . 12) .

	)	, , I K () 725/2004 31 2004, (L 129), .
		, . 12 2 . 3622/2007 (' 281), . 11 2 K () 725/2004, .
		(VTS), . 3) .. 49/2005 (' 66).
	)	, ; (12) 2 () 2015/962 18 2014, 2010/40/ (L 157), ,

		.
		(ITS), 4 . 1) .. 50/2012 (' 100).
3.		, . 1 4 () 575/2013 , 26 2013, () 648/2012 (L 176)
4.		, . 24 4 . 4514/2018 (14)
		, 2 . K 1) () 648/2012 4 2012, , (L 201).
5.		— , ' , . 3 . 4213/2013 (' 261).

		— 15 () 2022/2371 23 2022 A 1082/2013/ (L 314).
		— , . 1 2 .3/.. 32221/29.4.2013 , , , « .. , , . 2001/83/ « » (L 311/28.11.2001), 2011/62/, (L 174/1.7.2011)" (1049). — , 21 (NACE . 2). —

		( ) 22 () 2022/123 25 2022 (L 20).
6.		' , . . 1 2 1()/ . 27829/15.5.2023 , , , , « () 2020/2184 16 2020 (L435/1, 23.12.2020)" (' 3525), .

7.		, , , . 1, 3 , 2 2 . 5673/400/5.3.1997 , , , , , « » (' 192), , , .
8.		—
		— (DNS),
		— (TLD)
		—
		—
		—

		—
		—
9. ( )		
10.		' , . . 1 14 . 4270/2014 (' 143).
		...
		...
11.		, , , , .

II

A

(() 2022/2555)

1.		, . 1 . 2 . 4053/2012 (' 44), .

2.		, . 9 3 . 4819/2021 (' 129), .
3. ,		, . 9 14 3 () 1907/2006 18 2006, , , (REACH) 1999/45/EC K () 793/93 () 1488/94 76/769/ 91/155/, 93/67/, 93/105/ 2000/21/ (L 396), , . 3 3 , .
		, . 2 3 () 178/2002

4. ,		28 2002, , (L 31), .
5.	) in vitro	, . 1 2 () 2017/745 5 2017, , 2001/83/E, . (E) 178/2002 (E) 1223/2009 90/385/ 93/42/ (L 117), in in vitro , . 2 2 () 2017/746 5 2017, in in vitro 98/79/ 2010/227/ (L 117),

		( ) 22 K () 2022/123 25 2022 (L 20).
	) ,	26 NACE . 2.
	)	27 NACE . 2.
	)	28 NACE . 2.
	) ,	29 NACE . 2.
	)	30 NACE . 2.
6.		— /

		— /
		—
7.		

We order the publication of this in the Government Gazette and its execution as a law of the State.

Athens, November 27, 2024

The President of the Republic
KATERINA SAKELLAROPOULOU

The Ministers

National Economy and Finance
KONSTANTINOS CHATZIDAKIS

Deputy Minister of National Economics and Finance
NIKOLAOS PAPATHANASIS

Foreign Affairs
GEORGIOS GERAPETRITIS

National Defense
NIKOLAOS - GEORGE DENDIAS

Interior
THEODOROS LIVANIOS

Education, Religious Affairs and Sports
KYRIAKOS PIERRAKAKIS

Health Protection of the Citizen
SPYRIDON - ADONIS GEORGIADIS

MICHAEL CHRYSOCHOIDIS

Infrastructure and Transportation
CHRISTOS STAIKOURAS

Environment and Energy
THEODOROS SKYLAKAKIS

Development
PANAGIOTIS THEODORIKAKOS

Labor and Social Insurance
NIKI KERAMEOS

Justice
GEORGE FLORIDES

Immigration and Asylum
NIKOLAOS PANAGIOTOPOULOS

Social Cohesion and Family
SOFIA ZACHARAKI

Rural Development and Food
KONSTANTINOS TSIARAS

Shipping and Island Policy
CHRISTOS STYLIANIDIS

Tourism
OLGA KEFALOGIANNI

Digital Governance
DIMITRIOS PAPASTERGIOU

Climate Crisis and Civil Protection
KING KIKILIAS

State
CHRISTOS - GEORGE SKERTSOS

Deputy Minister to the Prime Minister
PAVLOS MARINAKIS

The Great Seal of the State was considered and affixed.

Athens, November 27, 2024

The Minister of Justice
GEORGE FLORIDES

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

The National Printing Office is a public service under the Presidency of the Government and is responsible for the compilation, management, printing and circulation of the Government Gazette (FEK), as well as for covering the printing and publishing needs of the public and wider public sector (Law 3469/2006/ÿÿ 131 and Presidential Decree 29/2018/ÿÿ58).

1. GOVERNMENT GAZETTE (GOVERNMENT GAZETTE) SHEET

• Official Gazettes **in electronic format** are available free of charge at **www.et.gr,** the official website of the National Printing House. Any Official Gazettes that have not been digitized and registered on the above website are also digitized and sent free of charge upon submission of a request, for which it is sufficient to complete the necessary information in a special form on the website www.et.gr.

• The **Government Gazettes in printed form** are available in individual sheets either directly from the Sales and Subscribers Department, or by post by sending an order request through the KEPs, or by annual subscription through the Sales and Subscribers Department.
The cost of a black and white Official Gazette from 1 to 16 pages is €1.00, but for each additional eight pages (or part thereof) it increases by €0.20. The cost of a color Official Gazette from 1 to 16 pages is €1.50, but for each additional eight pages (or part thereof) it increases by €0.30. The A.S.E.P. issue is available free of charge.

• **Ways to send texts for publication:**

A. Texts to be published in the Official Gazette, by public services and bodies, are sent electronically to the address **webmaster.et@et.gr** using advanced digital signature and timestamping.

B. Exceptionally, citizens who do not have an advanced digital signature may either send by post, or submit, through their representative, texts for publication printed on paper to the Department of Receipt and Registration of Publications.

• Information regarding the sending/depositing of documents for publication, the daily circulation of the Official Gazettes, the sale of issues and the current price lists for all our services are included on the website (www.et.gr). The website also provides information regarding the publication process of documents, based on the Publication Code Number (KAD). This is the number issued by the National Printing Office for all texts that meet the publication requirements.

2. PRINTING - PUBLIC NEEDS

The National Printing Office, responding to requests from public services and bodies, undertakes to design and print publications, brochures, books, posters, pads, computer- generated forms, folders for any use, etc. It also designs digital publications, logos and produces audiovisual material.

Postal Address: 34 Kapodistriou Street, Postal Code 10432, Athens	Website: **www.et.gr**
CALL CENTER: 210 5279000 - fax: 210 5279054	Information regarding the operation of the website: **helpdesk.et@et.gr**
PUBLIC SERVICE Sales -	Sending digitally signed documents for publication in the Official Gazette: **webmaster.et@et.gr**
Subscriptions: (Ground floor, tel. 210 5279178 - 180)	
Information: (Ground floor, Office 3 and call center 210 5279000)	
Public Material Collection: (Ground floor, tel. 210 5279167, 210 5279139)	Information about general protocol and correspondence: **grammateia@et.gr**
Opening hours for the public: Monday to Friday: 8:00 - 13:30	

Tell us what you think,

to improve our services, by filling out the special form on our website.